SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION	1b. RESTRICTIVE MARKINGS: NONE
AD-A219 182	3. DISTRIBUTION/AVAILABILITY OF REPORT: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.
S)	5. MONITORING ORGANIZATION REPORT NUMBER(S): AFIT/CI/CIA-89-170
6a. NAME OF PERFORMING ORGANIZATION: AFIT STUDENT AT Univ of CO/ Boulder	6b. OFFICE SYMBOL (If applicable):
	7a. NAME OF MONITORING ORGANIZATION: AFIT/CIA
6c. ADDRESS (City, State, and ZIP Code):	7b. ADDRESS (City, State, and ZIP Code): Wright-Patterson AFB OH 45433-6583
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable):
	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code):	10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO	WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification): (UNCLASSIFIED)
NETWORK SECURITY ISSUES

12. PERSONAL AUTHOR(S): MICHAEL JUDE SINISI

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
THESIS/DISSERTATION	FROM _____ TO _____	1989	148

16. SUPPLEMENTARY NOTATION: APPROVED FOR PUBLIC RELEASE IAW AFR 190-1
ERNEST A. HAYGOOD, 1st Lt, USAF
Executive Officer, Civilian Institution Programs

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL
ERNEST A. HAYGOOD, 1st Lt, USAF	(513) 255-2259	AFIT/CI

DD Form 1473, JUN 86 — Previous editions are obsolete. — SECURITY CLASSIFICATION OF THIS PAGE

AFIT/CI "OVERPRINT"

NETWORK SECURITY ISSUES

by

MICHAEL JUDE SINISI

B.S., United States Air Force Academy, 1982

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

Program in Telecommunications

1989

This thesis for the Master of Science degree by

Michael Jude Sinisi

has been approved for the

Program in Telecommunications

by

Russell E. Shain

Dale N. Hatfield

Hussain A. Haddad

Date 11/3/89

Sinisi, Michael Jude (M.S., Telecommunications)

Network Security Issues

Thesis directed by Dr. Russell E. Shain

The US is becoming an "Information-based Society" with telecommuniciations and computers increasingly being interconnected and interwoven in large networks with associated databases of proprietary and personal information. These networks and their associated databases are very valuable to society, providing easy, immediate access to information of all kinds. Business and the telecommunications industry are working to provide "easier" access, "more" information, and standardized protocols and/or translations, but there are costs and trade-offs to be made to the other side of this information revolution---security.

Network security is a current topic of concern, and needs to be addressed as we progress into the next decade. The trend towards more interoperative networks, computerized telephone networks, centralized databases make all of these very vulnerable to infiltration, alterations and destruction. Dangers to the networks come in various forms, from the network terrorist and the insider and the computer virus. Possible disruptive and

destructive actions and infiltration and exploitation of people's privacy rights. These dangers are present for all networks, but I believe there are a select few that are extremely critical to our health, welfare and security as a nation. If these networks were to be infiltrated and compromised, chaos could break out and hinder the government's ability to run the nation and/or the military's ability to respond to a crisis. Privacy concerns abound as telecommunications allow the creation of huge centralized depositories of information, shared databases resources with remote locations, all vulnerable to prying, unauthorized eyes. Stealing of data, blackmail, exposure of damaging information, violation of constitutional rights are only a few of the possible dangers to personal information located in databases. The dangers are real and we as a nation need to protect our sensitive networks and databases.

This thesis examines the security and privacy issues of the coming of the information age with its interconnected networks and centralized databases, and possible solutions to the dilemma. Technology and demand are driving forward with only cursorary actions being taken to protect the security and privacy of the

network, placing a number of highly critical networks in danger of being compromised.

DEDICATION

I dedicate this thesis to my parents who have believed in me and my abilities and have stood by me in my long journey to this point,

and to my new wife, whose encouragement, love, understanding and support helped me keep on track and focused on my goal;

and to my uncle Dr. Julio Torres for giving me the inspiration to go to college, complete my degree and to continue my academic pursuits and keep on learning, and for his love for travel.

CONTENTS

CHAPTER I

INTRODUCTION

Networking and network management are two of the "hot" topics in the telecommunications and computer industries. In the early 1980's personal computers became more powerful, user-friendly, and prevalent within our society, plus the divestiture of AT&T in 1984 enabled many entrepreneurs to enter the telecommunications business and compete. This fierce competition and pent-up consumer demand has led to the development of many new and varied telecommunications and information services. A recent government survey estimates that the number of these services has increased tenfold during the 1980's, and will continue to grow as telecommunications is a resource which increases in value as it becomes more widely available.[1] Industry also saw some dramatic changes as companies grew larger and larger, with many corporation mergers occurring, as U.S. industry began to compete on a global scale. Almost all businesses, government agencies and non-profit organizations now own computers (large, medium or small) or utilize data processing services.[2] The combination of these

changes made the idea of networking all of these computers via telecommunications lines very attractive. Networks began to grow and still are proliferating at an amazing rate in line with the dramatic increases in computer usage in the past decade. Some figures (US) are in 1986, 5.3 million PCs with 2.9 million of them networked together, and in 1994(est), 57 million PCs with 55 million networked together.[3] Industry has seen the value of interconnection, especially with remote sites, where there can be a centralized database and sharing of information and processing. The centralization of data and remote sharing over networks (public-switched and private) is less costly overall to the company and allows for easier access and use of information for the people who need it, whether it be many fixed sites or from mobile business and sales people all over the world. Industry has been spurred by the fact that business information and communications have become competitive tools needed for economic survival, and are no longer merely support functions.[4] Networking gives business flexibility in operations and the ability to expand and compete worldwide, while still maintaining a centralized corporate structure. Data transmissions from computer to computer can take

advantage of global time differences and spare processing capacity, as a result, the world has become a 24-hour competitive arena, especially in the financial and stock exchange services.[5] Demand for telecommunication and information services is so strong, that the international telecommunications and information market is expected to reach nearly $1 trillion by 1990.[6] Business will continue to develop new information systems and services and they will have a great need for information, and timely access to many types of public information (government and marketing information) that is widely scattered in different databases, thus making networking necessary and desirable.[7] Some examples of the potential new services include home banking, airline reservations, remote access to libraries, do-it-yourself newspapers, instant mail and video information services.[8]

Coming of the Information Age

The International Telecommunications Union (ITU) created the term *Telematics* in 1980 to describe this merger of the telecommunications and computer industries and the mass interconnection of computer data networks over telecommunications lines. Telematics is in its beginning stages and growing at a

rapid rate as networks proliferate and grow, especially with upgrades in the telephone network. The upgrade specifically being the replacement of electromechanical switches with electronic computer-switches and the upgrade of network lines from twisted wire to fiber optics. The telephone network currently carries the majority of digital information from computer to computer for public and private data networks. The basic premise of Telematics is the U.S. is "undergoing a fundamental shift in the economy that is moving from the industrial age to the information age".[9] The post-industrial information age industries surpassed, in value to the economy, manufacturing industries according to the Office of Technology Assessment (OTA), and they amounted to nearly 25 percent (as compared to 20 percent for manufacturing) of the U.S. GNP in 1986.[10] Information is now an economic commodity and a valued resource of any firm. The information storage and processing systems are growing in government and private industry, for example, the U.S. federal government maintains 3 billion records containing personal information in computerized record systems, according to an OTA report.[11]

Most companies today rely on computer systems to process and maintain information for

> inventory and engineering, accounting and billing, scheduling and reservations, maintaining personnel records, and many other functions.[12]

The keys in developing this information systems society are the rapid and dramatic growth in usage and technological advances in the telecommunications and computer industries.

The telecommunications and computer industries are merging in the area of technology, as evidenced by the new electronic switches whose controlling software comprises nearly 2 million lines of code.[13] Digital transmissions, while slow in speed, are commonplace with new, faster digital systems and networks being introduced today and development toward standardized networks for the future. Another technological improvement is the increasing use of fiber optic cable in the telecommunication networks. Fiber optic cables provide a high bandwidth with increased capability over traditional copper or coaxial cables for very high speed data transmissions. Currently, basic data services available include a 1.544 Mbps transmission rate, but with fiber optics rates in the gigabit range are possible. In addition, the U.S. already has at least four coast-to-coast fiber optic networks and a trans-Atlantic fiber optic cable, (with plans for another one by 1991), plus a fiber optic cable to

Japan by the end of this year.[14] All this has been made possible due to the vast increases in computing power and decreasing costs of computers and telecommunications networks and gateways over the past ten years. Personal computing power has increased dramatically with personal computers (PCs) today having the processing power of minicomputers of only a few years ago and of mainframe computers of the 1970's. Personal workstation computers are even more powerful, while barely larger than PCs, they are easily ten times as powerful.[15] In fact, A Sun SPARCstation 1 is able to execute 12 million instructions per second (mips), equivalent in processing speed to the IBM 3081mGX mainframe (a current model).[16]

> The technological revolution that has spawned the computer is creating a vast informational infrastructure encircling the globe--what can be thought of as a central nervous system for the planet. Resulting in a global organism that depends on information systems for its very survival.[17]

The reasoning for creating these networks is for the rapid and effortless sharing of information throughout society. This sharing of information is based on economics, flexibility, and efficiency in operations and control.

Social Aspects of Telematics

Technology, however, is not a neutral entity, there are social reasons for its development and implications in its implementation.

> Modern information and telecommunications technology cannot be properly understood if we persist in treating technology and society as two independent entities.[18]

The merger in telecommunications is desirable to large businesses and people who do much of their transactions between computers using modems or private networks. They could fully utilize the higher bandwidths and are willing to pay the high costs for this service and access to the multitude of information services and databases. My feeling is that the average person in America is not really concerned with the introduction of digital networks, such as ISDN; it will not have any immediate effect as most people would be hard-pressed to utilize the capabilities and will most likely retain their analog phones in the near term. People just will not see the need for a digital phone, plus the costs will be initially much higher than for the current service. In the information society, knowledge of computers and telecommunications may cause a severe social split, leaving parts of society technologically behind, and this gap may disappear or it may widen with future

generations. Knowledge is power, and its importance will only grow as more and more becomes available to everyone. Everyone, that is, that has the ability, skills and equipment to access and understand the information. This is especially clear today in the difference between the Western World and Third World. In the U.S. most of us do not think about what languages computers use, but the majority of computers use the languages of Western nations.

> Computers have always been the tools of cultural imperialism. To date they have never accepted any language other than English, Japanese or French, perhaps in exceptional cases.[19]

This is a real hindrance to the people without the skill or mastery of one of the "accepted" languages to have access to the wealth of information being offered. The analogy is clear, this type of division will occur as not everyone will have the tools or the ability to access this new world of technology and information. What many are touting as the beginning of paradise are very short-sighted and self-centered and are not really taking all of society into consideration. They may claim as such, but the reality of the situation is there is the distinct possibility of developing a "have" and "have not" pervasivness in society and in the economy.

Telematics can mean a higher standard of living, democracy, happiness---or equally, it can mean unemployment, repression and cultural impoverishment.[20]

America's evolution into a new information/service economy is continuing to experience rapid growth in overall numbers, with more private individuals having access to more information than thought possible in the past.

> The most revolutionary feature of the new means of communication is that many of them are interactive--permitting each individual user to make of send images as well as merely receive them from outside....all place the means of communications into the hands of the individual.[21]

Productivity, unfortunately, is not tied to this unprecedented growth, as office productivity has not kept pace with this influx of information technology. The US economy is growing and changing, but it does not necessarily mean a <u>qualitative</u> jump from one economy to another. The direct economic implications of networking and telematic technology are hard to define and predict as the market is still in a great state of flux from the unleashing of two decades worth of technology in less than a few years. It will take years for the long-term effects and trends to be felt, but one trend is clear, that telematics is

increasingly leading to a global market. The banking and financial institutions have already expanded worldwide and are dependent on current information from money markets around the world. Minor delays or disruptions in service could translate into substantial losses.[22] Business with the emergence of the multinational conglomerate has been working on expansion and interconnecting networks for the past decade.

Security and Privacy Issues

The concepts of interconnection and sharing of information over data networks of computers sounds great, but to only look at the benefits is tunnelvision.

> Now that the system (telecommunications network) has been improved, and its advantages widely proclaimed, the general public are virtually unaware of the reverse of the medal.[23]

The reverse of the medal is the security of the network and the integrity and privacy rights to the databases must be considered. Computer abuse and crime is increasing and must be dealt with, as the annual cost of computer crime has been estimated (1988) at $555,464,000, 930 person years and 15.3 computer years according to a census conducted by the

National Center for Computer Crime Data and The Racal Corp., both of Los Angeles.[24] Still more than half of U.S. businesses do not have a program of (computer) security to protect their confidential information, according to a survey by Lloyd's Corporate Security International.[25] In relation to database security,

> typical problems include the potential dangers to personal security and privacy which may arise from the combination of so many different databases within the integrated communal network....personal freedom in private life must be safeguarded against the threat of insufficiently confidential centralized archives with detailed information about individuals.[26]

Part of the problem is that society has moved so fast with the development and deployment of computer technology without due attention on how to protect those systems and it may now be extremely difficult if not impossible to protect those systems.[27]

Network security issues have caught the attention of the media, but for the computer industry, computer owners and many telecommunications and information systems managers, security is either a non-issue or one too difficult to face.[28] There are people that really do not believe in the possibility of a security breach of their system or that such a breach would be so minor that it does not warrant special (and costly) security measures. Basically, they do not believe the threat is real or that the

possibility of their system being infected are so remote. Currently many of the systems that are operating in industry and government were developed in the 1960's,'70's and early '80's. When these systems were developed little attention was placed on security, especially if the data to be stored or transported was not of a classified (in the military sense) nature. In the design and analysis phase of system development security should have been one of the top issues, but according to a Government Accounting Office (GAO) study, nine major U.S. government agencies failed to treat security as on the the system's integral functional requirements.[29] The agencies included the Internal Revenue Service, Social Security, Federal Aviation Administration, U.S. Customs Service, and International Trade Administration. Retrofitting older systems with security controls is a long, laborious and very expensive process that many companies cannot afford and sometimes cannot even be done.[30] There are countless systems with inadequate security controls, built in a time where the hacker was not a known threat. Also, these systems were designed to be extremely user-friendly, easy to use and access; a perfect invitation to disaster. But who would have

thought that someone would want to break into a hospital and look at patient records, for example?[31] The increasing use and interconnectivity put these systems at even greater risk that could have been imagined ten years ago.

Are network security issues relevant and what are the possible threats? And are their any options available? I feel these dangers are real, and will examine them in turn, but have limited the scope to the most important consequences of a "free and open" telematics society.

NOTES - CHAPTER I

[1] William G. McGowan, "Investment in Telecommunications: Opportunities or Pitfalls in Today's Environment," IEEE Communications Magazine, Jan 89, p. 30.

Daniel W. Latham, "Industry in Transition: Telecommunications-- Yesterday, Today and Tomorrow," IEEE Communications Magazine, Jan 89, p. 76.

[2] Alan F. Westin, "'We, the people' in the computer age," Computerworld, 14 Sep 87, p. 74.

[3] David Fawn, Telecommunications Seminar speaker from Southwestern Bell, Univ. of Colorado at Boulder, 5 Apr 89.

[4] Sir Eric Sharp, C.B.E., "Global Networks," IEEE Communications Magazine, Jan 89, p. 20.

[5] Delbert C. Staley, "Domestic Roadblocks to a Global Information Highway," IEEE Communications Magazine, Jan 89, p. 24.

[6] Staley, p. 24.

[7] Judith Irven, et al, "Multimedia Information Services: A Laboratory Study," IEEE Communications Magazine, Jun 88, p. 42.

[8] David D. Thornburg, "The Global Village Under Siege--We've Met the Enemy and He Is Us," Compute!, Mar 89, p. 13.

Robert S. Boyd, "Make way for computer shopping, private satellites and interactive videos," Daily Camera, Business Plus Section, 28 Feb 89, p. 13.

[9] Alan Baughman and Gerald Faulhaber, Telecommunications Access and Public Policy (Norwood, N.J.: Ablex Publishing Co., 1984), p. 6.

[10] Robert S. Boyd, "Into the Information Age," Daily Camera, Business Plus Section, 28 Feb 89, p. 12.

[11] "Government Data Bases and Privacy," The Futurist, Sep-Oct 86, p. 53.

[12] Irven, p. 28.

[13] Eric E. Sumner, "Telecommunications Technology in the 1990s," Telecommunications, Jan 89, p. 38.

[14] Danny E. Adams, "U.S. Telecommunications Policy: Directions for the Next Five Years," IEEE Communications Magazine, Jan 89, p. 44.

Boyd, "Into the Information Age." p. 12.

[15] Robert Wells, "Solbourne Computer seeks to create workstation standard," Daily Camera, Business Plus Section, 17 Jan 89, p. 10.

[16] J. Madeleine Nash, "Power Station in a Pizza Box," Time, 24 Apr 89, p. 51.

Kenneth C. Laudon and Jane P. Laudon, Management Information Systems, (New York: Macmillan Publishing Co., 1988), p. 182.

[17] William Halal, "Computer Viruses: The 'AIDS' Of The Information Age?" The Futurist, Sep-Oct 88, p. 60.

[18] Lars Qvortrup, Telematics, (Philadelphia: J. Benjamins Publishing Co., 1984), p. 7.

[19] Qvortrup, p. 177.

[20] Qvortrup, p. 1.

[21] Qvortrup, p. 36.

[22] Christopher Sterling and Stephen Thompson, "The United States in International Communications," in International Telecommunications and Information, ed. Christopher Sterling (Washington D.C.: Communications Press, 1984), p. 4.

[23] Qvortrup, p. 45.

[24] Newstrack, "Crime Statistics," Communications of the ACM, Jun 89, p. 657.

[25] "U.S. Business Falls Short on Computer Security," Computers and Security, Apr 88, p. 210.

[26] Qvortrup, pp. 45/49.

[27] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), p. 33.

[28] Gary Benbow, "Data Privacy - The Cost of Freedom," Computers and Security, Feb 89, p. 75.

[29] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), p. 5.

[30] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), p. 17.

[31] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), p. 46.

CHAPTER II

DANGERS TO THE NETWORK

The computer and associated network boom has been a great benefit for society, despite the detractions of some that they are impersonal, useless and a detriment to the human way of life. However, with every benefit for society there are those who will use it for criminal or malicious purposes. Computers are no exception. Computer crime takes many forms, including electronic stealing, "hacking", and the "newest" form, computer viruses.

Traditional hackers

Most people are aware of the phenomena of computer "hackers". They are stereotyped as over-zealous kids that break into networks to change grades, phone bills, make phone calls or do something to inform the people that their "secure" system is not as secure as they thought. While computer hackers could cause havoc, most of their impact has been relatively minor. Overcoming the challenge of breaking into the various networks is enough for them. The traditional hacker is giving way to more insidious

people who no longer are just "playing" in the network, but have some ulterior purpose. These can be people either inside or outside the organization, but one of their main weapons is---the computer virus.

Computer Viruses

Computer viruses are really not new, they have just increased in occurrence following the trends of increasingly more powerful and user-friendly computing and networking. Computer "viruses" have existed ever since computers were developed in the 1940's and 1950's. What exactly is a "computer virus"? In medical terms a virus is defined as an organism that invades the host body and replicates itself as it infects the host with its disease. Hence, the analogy was made to these small bits of computer programming that invade the host computer, replicating themselves and taking control, temporarily, of the computer. The virus also replicates itself onto any disks that it may happen to come in contact with. Viruses in and of themselves are not dangerous, it is only when they are "carrying a payload" that they become dangerous.[1] The payload can be a benign or malicious program. For the purposes of this dissertation, it will be assumed that

the term virus means a virus that is carrying some type of payload.

History

The first computer builders themselves began experimenting with programming discovered the virus, and played games with each other using these bits of hidden programming.

> The Core War was the brainstorm of three Bell labs programmers who recognized that computers were vulnerable to a peculiar kind of self-destruction. The machines employed the same core memory to store both the data used by programs and the instructions for running those programs. With subtle changes in its coding, a program designed to consume data could be made instead to consume programs.[2]

The core war involved having a number of self-replicating data-eaters battle it out in the computer's memory with the winner the one who had the most of their viruses occupying the memory.[3] This was a very controlled experiment, as the computers were stand-alone operations and could be shut down if the virus tried to spread into a place it should not. Plus only a few select people had access to the machine or even had the expertise to insert a program. The chances of having a viral infection were slim. With the advent of interconnectivity between computers this all changed, the virus could infect other machines and possibly get out of control before it

could be stopped.[4] Networking greatly expands the number of computers and databases that can be affected by these viruses. The effects of an unchecked virus "would be utterly devastating, since everything in this millennium-even our own identities-is connected to computers".[5]

Viruses were not a great problem during the 1950's up to the mid-1970's nor did any of the original virus inventors discuss the possibility of viruses.

> A self-replicating organism created in fun could be devastating if loosed upon the world of interconnected machines. For that reason the Core War combatants observed an unspoken vow never to reveal to the public the details of their game. But in 1983 Ken Thompson broke this vow, and even showed the audience how to write a viral program and stated, If you have never done this, I urge you to try it on your own.[6]

The late 1970's and 1980's have seen a boom in the development and proliferation of viruses. An important player in this is the development of the microcomputer with its relatively low cost and large amounts of power and ease of use; many more people have access to one than ever before. Equally important is the telecommunications revolution, which has greatly affected the ability of interconnecting these devices, and causing serious concern now and for the future. In fact, many computer manufacturers have

been stressing this basic point of enhanced interconnectivity to allow resources to be shared within an organization or all over the world.[7]

Technical Analysis

Before we discuss the virus specifically there are two related malicious data-eaters that pre-date and are related to their cousin the virus, and are part of the overall virus problem. The first is called a Trojan Horse. A Trojan Horse refers back to the story of the gift of a wooden horse by the Trojans that had quite a surprise inside. A computer Trojan Horse is a program that masquerades as an innocent and useful program, but has within it instructions to cause as much damage and destroy any data and program files it can access.[8] An example of a Trojan Horse was one that affected many Macintosh users in 1987. The program called "Sexy Ladies" deleted files as the viewers were pleasantly occupied with viewing the "program".[9] The programs can be cleverly disguised so that the unsuspecting computer user willingly follows the instructions, while the program is destroying their disk at the same time. A particularly diabolical example was a Trojan Horse that was attached to a program called "Flu-Shot IV", copied after the original "Flu-Shot" vaccine program.[10] The

program even mimicked the original commands, but by the end of the instructions instead of having a virus-free disk, the user's disk had been erased clean. The second malicious code is called a "time or logic bomb". This code hides in a computer until a certain date and time, at which time it becomes active and usually destroys data and program files. The Los Angeles Department of Water and Power had their mainframe IBM computer frozen by a such a "logic bomb".[11] Fortunately, the critical systems controlling water and power to the entire valley were not affected, but it still caused considerable and costly disruption for the Los Angeles municipality.[12] The key differences between these programs and codes and viruses are they usually do not replicate themselves or infect other programs as viruses do, and most Trojan Horses and logic bombs are planted from the "inside" of a computer system, while viruses are mainly an outsider type of infection.[13]

Technically, viruses are small streams of programming that can have enormous capabilities, sophistication and consequences.

> Viruses are hard to detect as they can take so many various forms, the only limit is the innovation of the designer, and a virus can do anything that other programs can do.[14]

Of course, your average user is not going to be able to create and launch a virus, it does take some programming knowledge and knowledge of the basic functions of various operating systems and how they store the data on the disks. But with that knowledge it is relatively simple to create a virus. Says, security consultant Ian Murphy, 28,

> Any decent programmer can write a virus within six hours, a novice can write one in 20 hours with assistance and 30 hours without assistance.[15]

An understanding of a disk structure though is necessary to understand how viruses work.

The common data disk contains 720 sectors, but it is the first twelve that are most important. The first sector, sector zero, (the boot sector) contains the disk parameter table (DPT), which specifies the number of sides, tracks, sectors per track and number of bytes per sector.[16] Sectors 1-4 contain the File Allocation Table (FAT) which

> is a roadmap of the disk's contents that shows where each file is located and the location of available free sectors. (Sectors 3 and 4 contain a duplication of this information).[17]

Sectors 5-12 contain the directory of the the programs on the disk. Data storage begins here unless the disk is a bootable systems program disk. In that case, the next 196 sectors contain the disks operation system,

and on a hard disk the structure may be more complex, but the initial sectors still contain the critical information.[18] This is the battleground for the viruses, the sites where they hibernate, and come to life. Destruction of these vital areas means the operating system cannot find any data or program files, it is as if the disk was a clean unformatted disk fresh out of the box.

Viruses are constructed to take advantage of the standard structuring of the disks. One particular virus was embedded within the command.com, and once the computer was booted and any command was activated to execute a program, copy a disk or ask for the disk directory the virus became active.[19] It then copied itself onto any uninfected command.com disk file, and when it had done this four times the virus wrote zeros on the first 50 sectors of the disk.[20] The critical first 12 sectors were now empty and the disk became unusable and valuable data or part of the operating system lost. The four new viruses that were created go and infect four more disks each and the virus increases itself exponentially. Another strain of virus transferred itself from an infected disk into RAM memory, where it would lurk infecting every disk entered into the machine during that session.[21] As

the person tried to execute any programs, the virus had already eliminated all information about the disk data and program files, (sectors 1-12) and none of the information could be accessed. A particularly ingenious virus that would attack vital clusters (two sectors equal a cluster) on hard disks and destroy sector zero on floppy disks, modified itself after being installed on someone's disk, therefore avoiding any viral detection programs.[22] The preceding viruses are all basically embedded within some type of executable code, (usually the operating system), but is it possible for them to be hidden within other programs and data files? The consensus is "yes", and these could be the most dangerous viruses of all.[23] If data files are all that is needed to spread the infection, this increases the vulnerability of networks that pass data and not executable code information, plus bypasses almost all anti-viral products.

Viruses are capable of almost doing anything as they are themselves an executable program. Most function to destroy or alter the first 12 sectors to make them unusable, as described above, but they can also write bad sectors onto disks (losing the data in those sectors), cause the disk to be reformatted, or

send all entering data to RAM so it is lost when the machine is turned off.[24]

Viral Classifications

There are basically two types of viruses, the first is a benign type, and the second a destructive type. The benign viruses basically may appear with a message or just overload the memory of the computer by its multiple replications. Perhaps the most famous three examples are the Macintosh Peace virus, the IBM Christmas tree virus and the recent case of the ARPANET virus. The Peace virus was one of the first public demonstrations of the exceeding ability of viruses to spread, plus the first case of a virus finding its way onto a commercial software product.[25] On March 2, 1988 a message of peace to all Macintosh users appeared on an estimated 350,000 machines around the world and then subsequently deleted itself, which is amazing since the virus was only unleashed two months previous.[26] The IBM Christmas tree virus spread from West Germany through the BITNET system as it sent a copy of itself to all addressees of a recipient and continued to do this, clogging the network over five continents.[27] The final example is the virus that infected the ARPANET. This virus was unique in many ways as it swamped the entire network

bringing everything to a standstill, yet no data was destroyed. This was not the first infiltration of the ARPANET by a virus. It was attacked by a moderately benign virus in the late 1970's, but it seems security was still lacking.[28] The virus quickly travelled throughout the network and plagued users for several days. The whole network had to be brought down and each user had to erradicate the virus or else the minute a virus infected computer was hooked up to the net, or a clean computer hooked up with the virus still travelling, the network would be reinfected. This virus showed how vulnerable our computer networks are and how a virus can have a life of its own. Countless times creators of virus underestimate the temerity of their creations and the little bugs become uncontrollable and a small experiment can become a catastrophy. Once a virus is launched, the creator has no idea where it will end up or how it will react to the software it encounters, and no amount of testing can verify it, as the virus becomes rambunctious and unmanageable.[29] The key with benign viruses is the originator is striving for attention, and the virus usually does no actual harm to the computer hardware, software and databases. The disruption though to the system and the cost of

erradicating make even these benign viruses a big and costly problem.

The second type is the one that is purposely malicious with the intent to wipe out a person's database, lock-up a computer or network with useless calculations or destroy their software or all of the above. This second type, or "data-eaters", are becoming more and more prevalant. The Lehigh virus destroyed countless disks throughout the university by wiping out the disk directories, and a similar virus was found on a network connecting about a thousand PCs at Hebrew University in Jeruselem.[30] It was designed to spread to as many computers as possible and wait until May 13, 1988 to delete all files. It was discovered due to a design flaw that caused the virus to replicate itself so much it significantly slowed down the computers' operations.[31] "Welcome to the Dungeon" were words embedded in the boot sector of a disk, a rare clue to the originator of a virus that has hit an estimated 100,000 IBM PCs throughout the US (and the world).[32] Actually the virus also included the names, address and phone number of the culprits. They were identified as two Pakistani computer programmers that had deliberately sabotaged the disks they sold to foreign tourists, especially Americans

out of their store in Lahore, Pakistan.[33] The "Pakistani or Brain" virus was hidden on bootleg copies of software that the brothers sold legally (in Pakistan) at cut-rate prices, and without warning to the users, the virus would scramble all the data on an infected disk, but only after spreading to other disks. The reason? The brothers felt that people that buy pirated software without paying copyright fees should be punished, but again this is a virus that got out of hand and spread all over the world wreacking havoc.[34] See Appendix A for a look inside the Pakestani Virus and its construction.

Vulnerabilities

So who is vulnerable to this mass plague? In reality, everyone is at risk, some have even compared this to the AIDS epidemic. While I feel it is not an apt analogy, it does serve to bring out how much attention and concern there exists today about these little "bugs". Anyone who uses or owns a computer is vulnerable to having that computer system infected, from microcomputers on up to the mainframes. Microcomputers are mainly at risk when people borrow, copy, lend or somehow introduce an outside contact to their computer's operating system software or any other software, (with some of the newer more

sophisticated viruses). A majority of infections come from the "shareware" available on public or club electronic bulletin boards or information services. This software is accessible and free for anyone who wants it, and usually includes useful programs, games--and viruses and vaccines!

> The most likely way of catching a computer virus infection is through electronic bulletin boards. Public-domain or share-ware programs are most vulnerable to tampering by unscrupulous hackers who might hide viruses in them or a program posing as legitimate may only be a cover for a travelling virus.[35]

Many people access these bulletin boards, infect their computers, infect a number of disks including disks they share with friends and disks that they use at work. Then they bring these infected disks to work, where the virus begins to really spread. Some companies have gone as far as to ban outside disks and contact with bulletin boards from company computers.[36] But this has a backlash of damaging the bulletin board and information systems that many programmers use for advertising and product distribution.[37] Even buying software at a legitimate store does not guarantee it will be free of viruses! (As with the Macintosh Peace virus).

Minicomputers and mainframes, the heart of corporate America, are also vulnerable to these minute

bits of data. However, many mainframe users disagree stating that the current architecture and security programs of a mainframe make it relatively immune to viruses, but I feel this is a false sense of security.[38]

> Just because only the lowly PC has been affected so far doesn't mean the more expensive and powerful minis and mainframes are immune. Where information can go, a virus can go with it, says Dr. Fredrick Cohen, a professor at the University of Cinncinnati who, for five years, has been doing research on the threat of computer viruses. According to Dr. Cohen, a mainframe can be subverted within an hour, and a computer network, including international ones with thousands of computers, can be overcome within a few days.[39]

The larger computers can be more vulnerable due to their high processing speeds. Why? An infectious virus can cause one of these large machines to speed up operations or replication of the virus itself and as the computer strives to do this, it starts to overload its own memory capacity. The virus can also cause the computer to wipe out its own memory and databases with its own lightning speed.

Many more cases are being disclosed with high publicity being given to the problem. Many experts feel that there were a number of cases of viruses severely affecting private companies operations, but were not disclosed to the public either due to ignorance as to what really caused the problem or for

fear of embarrassment or what a disclosure may do the the financial well being of the company and its stock. One computer firm, EDS, said that it sells security of a customers data and its reputation and very survival depends on it.[40] This is the reason many firms will not admit to a virus attack, what they did to counter it and their preventive security measures; "Would you leave your money in a bank that had its computer system corrupted by outside software?"[41] This follows the same pattern of many computer thefts and hacker infiltrations of the past.

Insider Threats

Many of the infiltrations are not really "break-ins", but the work of an "insider". An insider is someone with legitimate access to the computer system, who for one of many possible reasons decides to disrupt or destroy the system and/or steal data. The insider could be working for another nation or corporation, or it could be an act of vengeance of a disgruntled employee. This person may also do it for some political belief or the destruction may just be accidental. The motives are as varied as there are people, the key is, with insiders, they have the access and usually the knowledge to get around or

disable the security systems to cause their havoc. In 1985, the computer security officer of USPA, Inc. and IRA, Inc. was fired, but weeks before he had planted a destructive virus in the company's computer system. He returned after being fired, used a 'backdoor' password he planted to gain access and activated the virus which promptly erased 168,000 sales commission records. The virus was programmed to continue to delete records each month, but was discovered after a few weeks and eliminated.[42] In Congressional testimony, Mr. Thomas Giammo, Associate Director, Information Management and Technology Division, Government Accounting Office (GAO) summarized the insider threat,

> that the more serious damage is done by either current employees or by ex-employees. People who have detailed knowledge of the internal workings of the system and can get by the first kinds of checks and balances that have been put into the system.[43]

In addition he stated that in protecting a system, it must be well designed from the inside out, and that you identify and protect against certain employees who have a lot of access to the system, such as system programmers.[44]

Computer sabotage has become a greater threat since the USPA incident with the tremendous growth of interconnectivity. Part of the problem is many

information system managers are unaware of all the various interconnections of their own systems, and of all the various computers, software, and sharing of databases.[45] In the larger firms much of these acquisitions are done by individual divisions without the consultation or approval of the information systems manager. Companies have added systems, but one of the most dangerous is allowing dial-up interconnection. This can be a great benefit to allow employees to work from home or anywhere in the world, but it can also be a detriment if for example, a fired employee is barred from entering the building, but computer access via the telephone was not similiarly secured. Without complete information of all interconnections, and system hardware and software network security cannot become a reality.

It is also likely that a company employee could inadvertantly enter a virus into a network without knowing that his computer or computer discs are infected, with dire consequences. He could have acquired the virus in many ways, such as, accessing public electronic bulletin board programs (a favorite for virus creators), used their software on someone else's machine that was infected, or copied bootleg software that was infected. Unwittingly the employee

can become a courier of a virus, but while the corporate insider is currently responsible for the majority of all computer crime, I feel the threat with the potential for the most destruction in the new information age is one that is on the increase--the threat of "hackers" infiltrating networks and either planting computer "viruses" to spread throughout the computer interconnected networks or gleaning supposedly private/protected information from large databases. This new class of hackers I call "network terrorists". The fear of "terrorism" exists in industry where a company can launch a virtually untraceable attack on another to put them out of business, or use the interconnection to steal strategic plans, research data or personal data on employees. All this could be used against the firm, as

> security consultants hint at the possibility for blackmail; for sabotaging commercial rivals; for slow-moving, subtle, but devastating guerilla warfare against data banks; ultimately for an a attack by one nation's computers on another.[46]

Network Terrorist

A nationwide computer attack is a bleak and pessimistic scenario that is possible. What kind of person or country would do something like this? A malicious individual or country leadership trying to

further their own agenda at the expense of others with little respect for the consequences. How would this be accomplished? A "network or computer terrorist" or spy may be sent into a country, not necessarily the U.S., infiltrate their computer network and access any or all of our critical networks, spread a number of viruses into our system and/or steal valuable information. Foreign governments, corporate spys, career criminals and organized crime are becoming computer literate and have the resources to recruit and train terrorists.[47] Network terrorists could implant viruses programmed to replicate throughout various networks and wait years before activating. It is not that difficult!

> In early 1981, NSA officials working at an intelligence facility in suburban Washington made an alarming discovery: someone had made off with a sizable amount of classified information. The thief gained access to a "secure" cable leading into the facility and was able to trespass electronically.[48]

This thief could have easily planted many viruses. In fact, a virus programmed to destroy all data in the thousands of interconnected PC's at Hebrew University in Israel, on 13 May 88, the fortieth anniversary of the end of the Palestine state and birth of Israel, was discovered and neutralized before activating. Plus another virus was used to demand ransom in order

to obtain a vaccine to counter it potential effects.[49] Political terrorism is a realistic scenario. Instead of holding human hostages, companies and entire networks can be held hostage or destroyed. Valuable data may be stolen, often without the intrusion even being detected.

Both the CIA and NSA have experimented in disrupting other nation's computers with destructive viruses and have periodically broken into their computers to gather information.[50] The launching of a virus on a nation's most critical networks, whether research, financial or military could cripple that nation with consequences that could seriously affect the nation's economic, defense and social health. With the CIA and NSA playing games with viruses, it can be a safe conjecture that the KGB has also taken a keen interest in this area. The Soviets computing capabilities are on the rise, and there are electronic mail links to the U.S. giving them unprecedented access to U.S. information.[51] Most of the U.S. subscribers are currently corporations and scientific institutions, each with very valuable data, and possibly other network connections that could greatly profit a network terrorist. A recent study by the Swedish Ministry of Defense, concluded that Sweden's

sovereignty is at risk because of the increasing dependence on computers and telecommunications from a single computer (virus) attack.[52]

The dangers to the network are real. There are a multitude of forms and possible scenarios which these crimes may occur. Computer viruses with the greater connectivity in business and in the government can lead to a disasterous situation, especially if certain networks become the targets.

NOTES - CHAPTER II

[1] "Computer Viruses," The Colorado Engineer, Fall 1988, pp. 8-9, 16-17, as transcribed from "Watch Out For Viruses" by Carl Thor, in PC Transmission, Apr 88.

[2] Phillip Elmer-DeWitt, "Invasion of the Data Snatchers," Time, 26 Sep 88, p. 65.

[3] Elmer, pp. 65-6.

[4] Elmer, p. 66.

[5] "How Deadly is the Computer Virus," Electrical World, Jul 88, p. 35.

[6] Elmer, p. 66.

[7] David Thornburg, "Computer Viruses Use Networks to Spread the Disease of Distrust," Compute!, Jul 88, p. 10.

[8] Arlan Levitan, "The Trojan Wars," Compute!, Mar 88, p. 59.

[9] Suzanne Stefanac, "Mad Macs," Macworld, Nov 88, p. 93.

[10] Eliot Marshall,"The Scourge of Computer Viruses," Science, 8 Apr 88, p. 133.

[11] Jamie Murphy, "A Threat from Malicious Software," Time, 4 Nov 85, p. 94.

[12] Murphy, p. 94.

[13] Belden Menkus, "No vaccine to ward off effects of virus attacks," Computerworld, 11 Jul 88, p. 58.

[14] Bob Pontine, "Some common sense about network viruses, and what to do about them," Data Communications, Apr 88, p. 60.

[15] Murphy, p. 94.

[16] Dr. Harold J. Highland, "Random Bits & Bytes," Computers and Security, Apr 88, p. 117.

[17] Highland, p. 117.

[18] Highland, p. 117.

[19] John C. Dvorak, "Virus Wars: A Serious Warning," PC Magazine, 29 Feb 88, p. 71.

[20] Highland, p. 118.

[21] Highland, p. 120.

[22] Highland, pp. 120-1.

[23] "Computer Viruses," Colorado Engineer, Apr 88, p. 9.

Frank Ruiz, "DOD Fights Off Computer Virus," Government Computer News, 5 Feb 88, p. 77.

[24] Highland, pp. 121-2.

[25] "Nothing to Sneeze At," Time, 11 Apr 88, p. 52.

[26] Katherine Hafner, "Is Your Computer Secure?" Business Week, 1 Aug 88, p. 70.

[27] Marshall, p. 134.

"How deadly is the computer virus?" Electrical World, Jul 88, p. 36.

[28] Thornburg, p. 10.

[29] John Markoff, "'Virus' in Military Computers Disrupts Systems Nationwide," New York Times, 4 Nov 88, pp. A1 and A20.

"'Clever, Nasty and Definitely Antisocial'," Newsweek, 14 Nov 88, p. 24.

Phillip Elmer-DeWitt, "'The Kid Put Us Out of Action'," Time, 4 Nov 88, p. 76.

Linda Cornett, "CU students like doctors in finding computer cure," The Daily Camera, 5 Nov 88, pp. 1A and 10A.

[30] Thornburg, p. 10.

Marshall, p. 133.

[31] Pontine, p. 60.

[32] Highland, p. 120.

[33] Elmer, "Invasion of the Data Snatchers," pp. 62-6.

[34] Elmer, "Invasion of the Data Snatchers," pp. 62-6.

[35] Elmer, "Invasion of the Data Snatchers," pp. 62-6.

[36] Paul Karon, "The Hype Behind Computer Viruses: Their Bark May Be Worse Than Their 'Byte'," PC Week, 31 May 88 p. 53.

[37] Jim Seymour and Jonathan Matzkin, "Confronting the Growing Threat of Harmful Computer Software Viruses," PC Magazine (First Look), 28 Jun 88, p. 35.

[38] Karon, p. 53.

[39] Highland, p. 121.

[40] "How deadly is the computer virus?" Electrical World, Jul 88, p. 37.

[41] Seymour and Matzkin, pp. 34-5.

[42] Edward J. Joyce, "Time Bomb," Computer Decisions, Dec 88, p. 38.

[43] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), p. 16.

[44] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal

Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), p. 16.

[45] Joyce, p. 40.

[46] Eliot Marshall, "The Scourge of Computer Viruses," Science, 8 Apr 88, p. 134.

[47] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1985), p. 67.

[48] Jay Peterzell, "Spying and Sabotage by Computer," Time, 20 Mar 89, p. 25.

[49] "Fighting Parasites," The Futurist, Jul-Aug 88, p. 54.

[50] Peterzell, p. 25.

[51] Mark D. Berniker, "Electronic mail now links Soviets, U.S.," Daily Camera (Business Plus), 14 Mar 89, p. 9

[52] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1985), pp. 69/77.

CHAPTER III

COSTS OF OPEN NETWORKS AND DATABASES

Viruses, insiders and network terrorists all pose serious threats to the security and integrity of the nation's networks and databases.

The main networks and associated databases I feel could become prime targets are the Federal Reserve and banking networks, the stock exchanges network, the military classified and logistical networks, the government networks and databases and the research based networks, such as ARPANET. I believe these are most critical due to their implications to the economic health, welfare and security of our nation. Each of these networks carries with it a special place within our society that without them we would either not be able to function or further advance our knowledge.

Federal Reserve and Banking Networks

The Federal Reserve operates and maintains the financial well-being of the U.S. banking system. The system is considered to be so vital that it is regulated by the government. The Federal Reserve

network, referred to as FRCS-80, (later referred to as Fedwire) is a high speed data network that replaced the old Fedwire data network in 1983.[1] The system interconnects all federal reserve banks and branches, other financial institutions and many agencies of the government. Fedwire was a very vulnerable network, with minimal security, plus all transactions were processed and relayed by one central computer in Culpeper, Virginia. Any disruption to this computer or any of the lines leading to it could have been disasterous. The effect of a day's delay "would not only disrupt the nation's money supply, but would redistribute roughly $120 million in interest."[2] The Fedwire was a slower network operating at only 2400 bits/sec, but still responsible for transferring over $100 trillion annually, much of which used to be transmitted in essentially unprotected form.[3] The new network operates at 56 kbits/sec, is more secure from an outside attack and is decentralized with 15 hub processing points.[4] The network has no dial-in capability, encryption between links using encrypting techniques reminiscent of the military, which also prevents the interjection of spurious messages by the inclusion of a cryptographically protected message number or time stamp.[5]

While more secure, no system is totally secure from incursions, whether from the outside or inside. The consequences of a computer virus breaching this network would be ruinous, and the virus would not even have to be malicious, just the disruption and freezing of the system would be enough to send a panic throughout the financial world. Gold prices would soar and the entire economy of the U.S. and those multitude of economies that are invariably tied to the U.S. could crash, leading to world-wide economic chaos. An example of how just an innocent software problem (no virus) can affect the network occurred in 1985.

> When a software problem fouled up record keeping in Bank of New York's government securities trading operations in 1985, other banks temporarily stopped trading with it. The Fed (Federal Reserve) had to lend the bank $24 billion to keep operating until the problem could be fixed.[6]

Imagine what a virus could do!

Currently many methods including complex verification and authentication of data transfers, are used to prevent a break-in, but infiltration as mentioned above is not an impossibility.[7] Possibly the main threat could be from an insider, with legitimate access to the network, a disgruntled employee or someone paid to wreak havoc on the system.

The threat from insiders is considered by some to be a more serious threat, as NSA figures confirm that 90 percent of all known cases of computer security breaches are the work of corporate or government insiders, (This includes all kinds of computer crime).[8] The encrypted lines with time stamped messages are extremely difficult to overcome for the hacker, but they are of limited value against the dishonest employee who abuses his access to perform unauthorized acts. Most of the acts have been to steal money, some examples include, a chief teller stealing $1 million by using the bank's computer, a pay clerk used a military financial computer to steal $40,000, and an employee at a key federal agency stole $500,000 by using the computer to transfer funds.[9] These crimes involve financial gain, but a person wanting to disrupt or take down the network would just need access to the computer's operating system. Every computer has an operating system, many with thousands of lines of code, that can be easily infected with a hidden virus by an inside system programmer or other employees responsible for operating and maintaining the system. Some financial institutions are engaging in reselling their excess telecommunication and computing capacity, such as Citicorp, which needlessly

opens up their computer's operating system to attack.[10] These are the more serious threats, but fortunately they have not happened---yet. Terrorists have attacked many computer systems (including the financial network) in Italy, however, they did not do it electronically by computer, but used physical means (bombs, etc) to disrupt the systems.[11] The knowledge and tools for a more sophisticated attack are available today, and the terrorist will see a lot less risk in attacking a system with an insidious electronic bug from a distance.

The U.S. banking system also uses the Clearing House Interbank Payment System (CHIPS) to electronically transfer money all over the world. CHIPS handles billions of dollars daily, and like the Federal Reserve has experienced computer problems (but not viruses).

> In 1984, a computer error duplicated millions of dollars in payments, and John Lee, executive vice-president of the New York Clearing House that runs CHIPS, conceded that operational problems are always there; computers go down; software can have bugs in it.[12] In January 1987, the U.S. News and World Report magazine learned that the CIA had visited CHIPS to determine whether the Soviets could be penetrating it.[13]

While the CIA did not release its results, the concern was there, that the system could be vulnerable to sabotage, an act that could bring the system down, and

if it remained down long enough to seriously disrupt the economic fabric of the Western world. I do not feel that this scenario is either inconceivable or overdramatic. The world has become so dependent on computer speed electronic transfers, that slight mishaps could escalate and cause a chain reaction around the world. My concerns are shared by such notables as Felix Rohantyn, New York financier, John Kenneth Galbraith, the Harvard professor, and Gerald Corrigan, head of the New York Federal Reserve Bank (in 1987).[14] New Zealand's central financial transfer network has been hit twice with a computer virus, fortunately a benign virus just urging the legalization of marijuana, but the network was penetrated and is therefore vulnerable to data-eater virus[15] A more destructive virus that destroys data on hard disks has hit several major banks in London, Switzerland and West Germany.[16] The details of these attacks are not available, as vulnerabilities, security deficiencies are held in close secret to protect national security, the institutions and their reputations. These networks are not the U.S., but they do show criminals are penetrating supposedly secure financial networks. More and more sophisticated attacks could soon be expected, as PCs

and work stations increase in power and people become more computer literate.

Another financially related disaster is the possibility of one on Wall Street. A computer virus strategy here might be to tie-up the network or make it operate faster and faster. This could lead to a panic as experienced in October 1987. One of the problems with the stock market "crash" of 19 Oct 87 was the tying of the buying and selling of orders to computer programs. Once started, the selling just increased at an exponential computer-like speed, and the result was the temporary collapse of the market. The stock market is a very sensitive part of the world economy and literally influenced by almost everything happening in the world today, especially political or economic turmoil. A run on the market caused by a virus, whether for the plus side or down side could also bring the economies of the world to their proverbial knees. According to the New York Fed, Wall Street's average daily volume of wire transactions totals at least $1.2 trillion and could be as much as $500 billion a day higher.[17] Security of this network also extends to protecting the databases of information on ownership and possible plans outlined by large companies on future deals and strategies. A

person able to infiltrate a database of Merrill Lynch or any other brokerage firm could gain valuable "inside information" to use illegally to either further their own gains or even to destroy a company by feeding the information to its competitors. This is especially true in the current era of mergers and leverage buyouts. Inside information would be very valuable for stock and price manipulation.

Government Networks

Military

The Department of Defense (DOD) computer and telecommunications networks are responsible for the security of the nation. The DOD has many, many different computer networks that are part of the Defense Communications System (DCS), including the Automatic Digital Network (AUTODIN) and the Defense Data Network (DDN), and thousands of microcomputers (PCs) that are being increasingly interconnected via local area and wide area networks, and most travel the nation's public telephone networks. The implications here are obvious, infection with a virus could pose serious problems in the military's ability to meet their mission in defending the country. There was even a movie about a boy that infiltrated the defense

department network and nearly started a nuclear war ("War Games" MGM/UA). While that scenario is highly unlikely, a "computer terrorist" could severely cripple our ability to respond to a crisis with a loss in time and ability. Part of the film was even shown as the prelude to Congressional testimony on computer security and privacy.[18] The classified computer networks are assured to be unaccessable and safe, because they are not connected to the public network (via dial-up connections). Also, these networks are protected by bulk encryption of all transmissions, whether or not the data being transmitted at the time is classified. The encryption devices are the best in the nation (and probably the world) developed by the National Security Agency (NSA). As computer experts agree, no computer system is completely impenetrable, and given the increasing reliance on computer systems for defense, the threat of enemy infiltration and sabotage will only increase. General John A. Wickham, Jr. (Ret.), President of Armed Forces Communications and Electronics Association, believes in the potential threat a network terrorist poses to national security, stating,

> Our daily lives and national security are too reliant on automation and communications networks for us to avoid the hard choices (expensive and less friendly to use systems)

> associated with information security. Given mankind's history, it does not take much imagination to anticipate that some future software programs in the hands of malicious individuals could become virulent forms of terrorism.[19]

These classified data networks, such as AUTODIN, are fairly secure against an outside attack, but there is always the other danger of the "insider" stealing from and disrupting the network. The military performs security checks on all individuals that will have access to classified information, and these are now reinvestigated every five years for Top Secret access. This is to try to determine the trustworthiness, reliability of people given access and to ensure there is nothing in their background that could lead them to compromise their integrity. An immense number of people who work for the military, federal government and defense contractors hold security clearances and recently the number of people cleared and the level of clearance allowed have both been reduced. This was in response to the Stillwell Commission, which was established after the Walker espionage case to investigate security standards within the federal government.[20] The Walker case involved the stealing of naval classified information and cryptographic codes by cleared individuals, John Walker and Jerry Whitworth. The Stillwell Commission

emphasized personnel security stating there were little controls on security clearances, that they were given out without any real consideration, and basically people that had them had no need for access to classified information in their jobs. Personnel security "has always been the weakest link in any security system."[21] With the multitude of personnel that have clearances, the potential for an insider to penetrate the network is enormous. Recent cases of alleged espionage and defection to the East have been well publicized in the media, and the reasons are as varied as there are people. The military is trying to crack down on leaks and potential disasters, but the possibility of a cleared individual taking huge amounts of classified data out on a floppy disk (much easier than the previous paper files) or entering a virus on a critical network, such as the WWMCCS (World-wide Military Command and Control System) does exist. Robert Brotzman, director of the Department of Defense Computer Security Center at Ft. Meade, MD, said:

> That the techniques of today's computer thieves are too sophisticated and the targets are too inviting to ignore. Considering how much fun the bad guys could have on U.S. computers, if they ain't having at them, they're a lot dumber than we think they are.[22]

The Defense Data Network (DDN) has expanded enormously in the past few years and is continuing to grow. The DDN is a packet switched network, that allows subscribers to connect via terminal access (ie. PC) via a terminal access controller using a modem and dial-up access from anywhere in the world.[23] The system also features interconnection with multitudes of local area networks within the DOD, gateways to other DOD (unclassified) and government networks with such operations as electronic mail, file transfer and distributed transaction processing.[24] The dangers are clear, the operations allowed are the perfect grounds for the interjection of a virus. The computers that allow the distributed processing are enabling the hacker access to the vital controls and operating system of the computer. The network is so large and growing that a virus infection could cause severe disruptions. The DDN is an administrative data network with no classified interconnections, plus is not be considered a critical command and control network, so the damage to national security would be limited, but the damage during peacetime operations would be formidable.

The military's unclassified logistical network is also at risk as the military is using more PCs for

end terminals. The system also is has dial-up capability making it accessible from almost any phone, (a very dangerous capability) and does not use encryption techniques.[25] The logistical network is critical for day-to-day operations, plus in wartime it is the military's key for staying in battle.

> A different virus is introduced into NATO's logistic computers. Triggered just as the Soviet army marches into West Germany, the virus alters messages so that all allied supplies are sent to the wrong places. By the time it is corrected, key parts of NATO's defense line have collapsed.[26]

A realistic possibility. While the logistical network does not carry any classified information, it does carry sensitive information from which an enemy may be able to use to ascertain current mission readiness and capabilities. If for example, a radar unit orders a key component, the ability for this unit to perform effectively may be in an impaired status; very valuable information for an enemy planning an attack.

In addition to these networks, personal data/sensitive information is being increasingly and routinely being transmitted from computer to computer (PCs) using such insecure systems as electronic mail, (E-mail) over unencrypted public lines. This information contains personnel performance data (good and bad), social security numbers, and other personal

record information. The system installed in the 601st Tactical Control Wing, Sembach Air Base, West Germany was designed to interconnect many remote units all over W. Germany that report their personnel data to Sembach's personnel center. The system consisted entirely of either Burrough's word processors and Zenith Z-100 computers, all PCs, located in relatively insecure offices (just locked doors with numerous people with keys). A person's privacy could easily be breached by people unauthorized to see the information.

The DOD does believe the threat to its systems and networks is real. In fact, in a communique released in early 1988, from the Office of the Assistant Secretary of Defense, a question posed as to whether computer viruses are a concern to defense computer systems, the answer was "yes, its (the virus) potential threat is severe."[27] The military also has a comprehensive security training and awareness program and is in the process of tightening security loopholes. For the military, the posture is that the enemy is always watching and listening and everything must be done to prevent a compromise, even if it means less user-friendly systems. There have been compromises, some very serious, but the prevailing

attitude is very different than the one in the rest of the government and commercial sectors.

Civil Agencies

The Federal Reserve and DOD networks are all part of the federal government, but in addition to these networks, the civil part of the government is also automating and using more networking and interconnections to improve their capabilities. The federal government is in fact the largest user of telecommunications in the nation; its very operation and life depends on being able to communicate with lower agencies and visa versa. The government maintains about 85 major different databases containing some 288 million records on 114 million people, nearly 48 percent of the population.[28] Also, the General Services Administration (GSA) estimates the government operates over 20,000 mainframe computers at over 4,500 sites and expects by 1990 to have more than 25,000 mainframes and over 500,000 PC computers installed and operating.[29] These numbers were estimates made in 1985, and I feel the government may have many more PC computers today because it has been so easy to obtain PCs. After the contracts were let by GSA, each agency was free to purchase as many

PCs within their budget, but when ordering, installing and using the agencies rarely consider security.

> The prolific growth of office automation and PCs within the federal government is another area of concern, as little consideration has been given to the security aspects of these stand alone and netted systems.[30]

A few of the major systems include the Internal Revenue Service (IRS), the Social Security Administration (SSA), the Federal Aviation Administration, the Federal Bureau of Investigation (FBI), and Veterans' Administration. On May 19, 1988, Thomas Giammo, then Associate Director of the General Accounting Office's (GAO) Information Management and Technology Division, said that information system security in the U.S. government civilian agencies was seriously inadequate, and he noted there was a persistent failure to include security considerations throughout the system development process, and an apparent lack of managerial concern with computer security.[31] Many agencies feel that the information they deal with in not classified in the military sense, and why would anyone want to access it anyway. That is the attitude that enables hackers to begin with accessing these systems that are relatively insecure and innocuous, and wreak havoc while they learn how to enter more difficult systems. Security

should be considered during the entire ordering process, as this was not the case years ago. Many of the systems installed today are "antiquated", with many different vendors' hardware and software, and very difficult, if not impossible to secure. In some cases it may be cheaper to buy a totally new system than to try to install patches and add-on equipment for security. The government realized the potential threats posed by insiders, hackers and viruses and has taken action in the form of legislation, Presidential directives, agency directives and training programs to try to improve security and increase threat awareness. The effectiveness of the programs and government actions are open to debate.

Research Networks

The U.S. operates many vital research networks, which include many of the science and research centers located all over the nation, including the Advanced Research Projects Agency Network (ARPANET). ARPANET includes major universities, military installations, and major organizations, such as NASA, Lawrence Livermore, SRI International, and the Naval Ocean Systems Command.[32] The net was created to facilitate the exchange of

research data throughout the academic and scientific communities. Is it a vulnerable network? A rhetorical question since on 2 Nov 88 it was proven to be vulnerable to infiltration by a relatively benign computer virus, and on 3 Mar 89 infiltration by computer hackers.

The 2 Nov 88 virus was launched by Robert Morris, Jr., a graduate student at Cornell University and son of Robert Morris, Sr., chief scientist at the National Computer Security Center.[33] The virus travelled throughout ARPANET, Military Network (MILNET) and National Science Foundation network (NSFnet) infecting over 6,000 computer systems, bringing the entire network down as users disconnected from the network until they could be sure the virus had been completely erradicated. The virus operated by taking advantage of flaws in the UNIX operating system software. It was an ingenuous multifaceted attack using the "finger" program (used to gain information about other users), the "sendmail" program (designed to route mail throughout the network) and breaking passwords.[34] The passwords on the systems are encrypted using a standard algorithm, but the virus used the account name and variations of them, then a list of 432 built-in passwords and finally all

the words from a dictionary as potential passwords, encrypted them (as an "authorized user"), and compared them to the encrypted passwords in storage.[35] Some sites reported that over 50 percent of their passwords were compromised using this approach due to the use of common words as passwords.[36] The virus once it gained entry would use the mailing lists of the attacked computer to further promulgate itself, but it was very clever in deleting where it had originated from, in fact the virus disabled the operating function that would cause a memory dump for audit analysis.[37] Morris developed the code as a 99-line penetration shell with a 3,000 line C language program which contained the actual virus code, but he most probably did not expect it to get out of control like it did nor that one in every seven viruses would declare itself "immortal" and refuse to terminate itself if it ran into another virus attacking the same computer, as programmed.[38]

It took computer experts working all over the nation days to finally "catch" the virus, decompile it and analyze the results to determine how the virus attacked systems, how it was able to hide itself so well, and finally how to stop it. The virus did make the general public aware of the dangers of open and

interconnected networks, even though they were not really affected. The virus did affect the attitude for which the ARPANET was designed for, sharing of information, ideas and programs and research data. Most of the users were already aware of the flaws in security, but accepted them as a part of an open network.[39] The researchers were relying on the ethical behavior of all participants not to exploit these flaws. For a network terrorist these flaws could benefit him in two ways, either launch a destructive virus or just log on and gather some very valuable research data.

Why the importance of this network attack? A malicious virus could have destroyed extremely valuable research data. Many a person's life work could have been wiped clean in a matter of seconds. The US military depends on its technological edge to counter the overwhelming superiority in numbers of the Warsaw Pact forces. Plus in industry, our economy depends on staying on that "leading edge of technology" to be competitive in the world markets. Much of the academic and scientific research also crosses boundaries between the private and public sectors and is of benefit to all mankind. The scientists need the free access and exchange of ideas

and research in order to function and make those "breakthroughs". The network is still vulnerable, as West German computer hackers gained access to the network and obtained valuable programs, information, plans, technological discoveries and theories and many other valuable data. Not so serious until their "employer" was named--the USSR; they sold the information to the Soviet Union.[40] Espionage cases occur everyday, but very few ever become public knowledge; that is the nature of the business. When a case does become public, it can signal a serious breach in security, one that cannot be hidden from the media and public scrutiny. One such celebrated case involved West German hackers infiltrating various computer networks in the U.S. and allegedly penetrated defense contractor and research computers and stole valuable information---the 3 Mar 89 ARPANET infiltration. The case began with a minor discrepancy in a bill at the Lawrence Berkeley Laboratory, but Clifford Stoll, an astronomer and computer expert saw the 75 cents as a major breach in security.[41] The FBI turned down his call for help and he proceeded on his own, and eventually tracked down the hacker after 18 months.[42] In the 18 months the hacker tried to break into over 450 computer systems, being successful in

over 30 systems.[43] The main systems he tried to enter were located at military and research installations including NSA headquarters, Army bases in Alabama and Georgia, Navy bases at Norfolk, VA, and Panama City, FL, defense contractors, Mitre Corp. and Unisys, and the Jet Propulsion Laboratory in Pasadena, CA.[44] The hacker would look for military sounding data titles and download as much information as possible, and allegedly sold it to the USSR. The compromised systems included computers at NASA, the DOD Optimus database (contents unspecified), a computer at the Los Alamos National Laboratory, and various military and research computer systems in France, Germany, Holland and Italy. The information taken from U.S computer systems included sensitive, but apparently unclassified data on the U.S. nuclear and biological capabilities, plus many passwords to other DOD systems, and valuable research data and software.[45] A major blow to the West's technological edge was the designs for a 1 megabit chip and sophisticated design software from the Thomas Company of France and N.V. Phillips of Holland.[46]

Network security has not been a top priority on the ARPANET, with the research centers relying on the trust and integrity of the associated members, and

while they have said that security has been tightened, it will still be a prime target for infiltrators.

> Five weeks after a computer science student forced the Defense Department to shut down its ARPANET computer network, the Pentagon learned that one of its smaller military information systems, MILNET, had been broken into.[47]

The hacker had gained access through the Mitre Corp. (a defense contractor) through an ARPANET link.[48] The Pentagon severed MILNET's connection to ARPANET until a software fix could be found.[49] Again it must be noted these very networks were designed with that free exchange of information cornucopia with no inkling to possible hazards. Although, the collected information could be very damaging to the research programs in the US and the security of our nation. It is quite a dilemma.

ARPANET is not the only research network to be compromised, in 1987, hackers gained access to the Space Physics Analysis Network (SPAN), a worldwide network administered by NASA.[50] SPAN is a library of space-related information, which includes an E-Mail function, and is not interconnected with any classified systems. The hackers claimed to have entered 135 computer systems around the world and as having extracted a wealth of information on the space shuttle, strategic defense initiative and other

topics, a charge NASA denies.[51] The hackers even planted a virus (trojan horse) to make the system easier for others to access, plus publicized how to break into the network, including passwords, on a New York computer bulletin board.[52] Security was lacking, but as with the ARPANET, the system was designed for free flow of information rather than security. NASA said that there was no real damage done, just embarassment, but with that kind of attitude, it leaves the door open for the malicious individual to launch a virus and destroy data and bring down the network.[53]

Privacy Concerns

Privacy has also become a central issue in network security as the military and the government have many databases of information that are slowly becoming interconnected and centralized. The databases are being merged to share information, plus it can be more economical to have a centralized database to ensure that all programs and computers will be interoperable, and all information in each section/agency is the same and current. The information could be unclassified as it stands separate, but cross-referenced or merged with other

related sensitive data could make the information classified and in need of higher protection. Sensitive data about individuals gathered by the government and cross-referenced could be used beneficially in helping tracking down hardened criminals, tax evaders, or missing children, but there is the fear that it could be accessed by people and used for other than legal purposes, possibly blackmail.

> The increased centralization of information storage also makes possible concentrations of power both within central government offices and in larger private business.[54] Information technology is the incarnation of fears about the oppression of the individual and the fears about police surveillance and thought control.[55] Authorities and large private concerns have an interest in monitoring some individual activities, and the new technology provides them with the means to do it. Our private lives will be threatened, because our political attitudes, financial transactions, selection of information or entertainment, etc, will be automatically registered.[56]

In other words, as the files stand separate no one can get an entire profile of an individual, but centralized anyone accessing the system can get that "picture" and discover certain information that may be very sensitive in nature, such as history of mental health treatment, financial data, sexual preferences, credit history, drug use information or previous names or marriages. Much of this is available in public

records, but in many separate files and agencies where access is usually a long and arduous process. In April of this year, the city government of Santa Monica, CA, opened up their public records and files via a modem and a computer or one of 20 public terminals set up in libraries and recreation centers. The system called Public Electronic Network or PEN discourages sabatoge by hackers by making all users pledge to use PEN for only legal purposes nor to change or destroy any data.[57] Some security system! It is an open invitation to disaster.

Part of the privacy invasion involves the use of a person's social security number as a universal identifier. The government, federal and state, in most cases rely exclusively on the social security number for tax identification, motor vehicle registration, health and welfare benefits, and criminal activities. In the military, the old standard identification serial number has been replaced by the social security number. In the private sector, credit bureaus, banks, insurance companies, employers all have begun to use the social security number as a handy identifier. Why all the fuss about a number? Well, as a universal identifier, it makes it much easier in the information age to

cross-reference and match records to gain that overall profile both within the government and commercial sectors. The IRS uses the number to catch tax evaders, the SSA uses it to catch people cheating on benefits, in fact, government databases form the most cohesive web of information on individuals: some 15 agencies mix and match data.[58] And the number is expanding, according to Pricilla Regan, an analyst with the OTA, the U.S. is moving toward a national database.[59] Two of the biggest users in the commercial sector are credit bureaus and medical referral services. Credit bureaus can instantly give the credit and financial history of a person using the social security number identifier and until recently they were given access to the IRS computer database. Many companies, retail stores, banks and the government uses them to verify applications for loans, jobs, and financial stability for purchases.[60] The medical service offered by Docket Search Network Inc of Chicago, "consists of information on patients who have filed civil suits (patients to avoid or watch)."[61] Other companies are expanding into compiling databases on court action taken by tenants to be purchased by landlords (tenants to avoid or watch), and census information for marketing purposes.

Most of these databases use the social security number as the identifier, which makes interconnection more and more revealing about information and preferences on individuals. This information may be used to make decisions about a person's life, without knowing that all this information has been accessed or even whether it is all correct. Also, the information may be used to harm, extort or embarrass individuals as in the case of a hacker who gained access to the TRW credit reporting database, and found information (small claims court collection suit) about a local candidate for public office and made that information available to the media with damaging results.[62]

Privacy is a real concern as we enter the information age, numerous congressional hearings have been held to discuss this very issue. It all draws back to the issue of security. These databases need to be secured against people infiltrating and rummaging through them to glean sensitive, private and potentially damaging information for unauthorized uses. People also need to know about the files so that they can ensure that the information is accurate and complete. The threat of interconnected databases, brings to mind the "big brother" syndrome from George Orwell's book *1984*, where the government has total

control and there is no individual privacy. Critics warn that computerized data systems in government, collecting and integrating millions of personal records on citizens, could result in a massive loss of privacy, denial of due process and chilling effects on personal expression and dissent.[63] The Federal Bureau of Investigation (FBI) operates the National Crime Information Center, which has more than 10 million centrally stored records of criminal histories all available to authorities nationwide.[64] The fears being one of a police state and loss of freedom and privacy. It is also seen as a potentially dangerous increase in power for a police agency.[65] The Secret Service is reported to be building a system to help identify potential assassins, and most likely using connections to government databases to accomplish their goal.[66] They could also be trying to access public library records to see which individuals were interested in books considered subversive, something the FBI tried to do, but were denied by the courts. Security and privacy, threatened by the information age technology and the malicious users of the new technology and interconnected networks, but all is not lost.

NOTES - CHAPTER III

[1] J. G. Martin, "Federal Reserve Communications System Planning," IEEE Journal on Selected Areas in Communications, May 84, pp. 395, 401.

[2] Martin, p. 398.

[3] Jason Gait, "Communications Security for Electronic Funds Transfer Systems," IEEE Journal on Selected Areas in Communications, May 84, p. 414.

Martin, pp. 396, 397.

[4] Martin, p. 400.

[5] Gait, p. 420.

[6] Katherine Hafner, "Is Your Computer Secure?" Business Week, 1 Aug 88, p. 65.

[7] Patricia Keefe, "It can't happen here....," Computerworld (Focus), 6 Apr 88, p. 13.

[8] Jay Peterzell, "Spying and Sabotage by Computer," Time, 20 Mar 89, p. 25.

[9] August Bequai, Esq., The Cashless Society: EFTS at the Crossroads, (New York: John Wiley & Sons Publishing Co., 1981), p. 68.

[10] Henry Geller, "Telecommunications Policy Issues: The New Money Delivery Modes," in Electronic Funds Transfer and Payments: the Public Policy Issues, ed. Elinor H. Solomon (Boston: Kluwer Nighoff Publishing Co., 1987), p. 71.

[11] Bequai, p. 72.

[12] Monroe Karmin with Pamela Sherrid, "Risky Moments in the money markets," U.S. News and World Report, 2 Mar 87, p. 45.

[13] Karmin, p. 45.

[14] Karmin, p. 44.

[15] Jack Wynn, "Meeting the Threat," American Banker, 2 Feb 89, p. 8.

[16] Wynn, p. 8.

[17] Karmin, p. 44.

[18] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), p. 13.

[19] John A. Wickham, Jr., "Protecting Our Computers," Signal, Jan 89, p. 19.

[20] Thomas J. O'Brien, "The Changing Face of DOD Security," Security Management, Jul 88, p. 62.

[21] O'Brien, p. 62.

[22] Richard Sanza, "Spying through Computers?" Newsweek, 10 Jun 85, p. 39.

[23] Dr. William Stallings, "Interfacing to the Defense Data Network," Signal, Aug 88, p. 103.

[24] Stallings, pp. 104, 107.

[25] Sanza, p. 62.

[26] Peterzell, p. 25.

[27] Office of the Assistant Secretary of Defense, "DOD's 4 Year Virus Program," Computers and Security, Oct 88, p. 446.

[28] Anne Field, et al, "'Big Brother Inc.' May Be Closer Than You Thought," Business Week, 9 Feb 87, p. 84.

[29] U.S. Cong., House Subcommittee on Transportation Aviation and Materials and the Subcommittee on Science, Research and Technology of the Committee on Science and Technology, Federal Government Computer Security, Hearings, 99th Cong. 1st sess., (Washington, D.C.: GPO, 1986), pp. 58, 86.

U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), p. 87.

[30] Lawrence Castro, "An Overview of the DOD Computer Security RDT&E Program," Proceedings of the 10th National Computer Security Conference, 21-24 Sep 87, p. 264.

[31] Belden Menkus, "U.S. Government Agencies Belatedly Address Information System Security Issues," Computers and Security, Aug 88, p. 361.

[32] John Markoff, "'Virus' in Military Computers Disrupts Systems Nationwide," New York Times, 4 Nov 88, p. A20.

[33] Peter J. Denning, "The Science of Computing," American Scientist, Mar-Apr 89, p. 126.

[34] Eugene H. Spafford, "Crisis and Aftermath," Communications of the ACM, Jun 89, p. 678-9.

[35] Denning, p. 126.

[36] Spafford, p. 680.

[37] Denning, p. 126.

[38] Denning, p. 126.

Ted Eisenberg, et al, "The Cornell Commission: On Morris and the Worm," Communications of the ACM, Jun 89, p. 707.

[39] Severo M. Ornstein, "Beyond Worms," Communications of the ACM, Jun 89, p. 672.

[40] Peterzell, p. 35.

[41] Eliot Marshall, "German Computer Spy Ring Broken," Science, 24 Mar 89, p. 1545.

[42] Marshall, p. 1545.

[43] Steven Dickman, "Hackers revealed as spies," Nature, 9 Mar 89, p. 108.

[44] Dickman, p. 108.

[45] Evelyn Richards and R. Jeffrey Smith, "Hacker tracker followed trail across Atlantic," Daily Camera, 4 Mar 89, p. 11A.

[46] Marshall, p. 1545.

[47] "Another Infection," Time, 12 Dec 88, p. 33.

[48] Neil Munro, "Feds say Hackers Invaded Three Defense-Related Systems," Government Computer News, 19 Dec 88, p. 6.

[49] "Another Infection," Time, 12 Dec 88, p. 33.

[50] William D. Marbach et al, "Hacking Through NASA," Newsweek, 28 Sep 87, p. 38.

[51] Marbach, p. 38.

[52] Marbach, p. 38.

[53] Marbach, p. 38.

[54] Lars Qvortrup, Telematics, (Philadelphia: J. Benjamins Publishing Co., 1984), p. 45.

[55] Qvortrup, p. 33.

[56] Qvortrup, p. 74.

[57] "Plugging Into City Hall," Time, 6 Mar 89, p. 33.

[58] Field, p. 84.

[59] Field, p. 85.

[60] Field, p. 85.

[61] Field, p. 85.

[62] Douglas E. Campbell, "The Intelligent Threat," Security Management, Mar 89, p. 19A.

[63] Alan F. Westin, "'We, the people' in the computer age," Computerworld, 14 Sep 87, p. 75.

[64] Field, p. 85.

[65] Westin, p. 77.

[66] Field, p. 86.

CHAPTER IV

POSSIBLE SOLUTIONS

The future looks grim for networking and computing, to avoid a catastrophe, network security needs serious attention, and solutions to the potential dangers must be implemented now. How can society ensure network and data integrity without seriously infringing on the rights of individuals to have access to information? There are many varied possible solutions and protection measures, but these alone may be effective against only certain specific dangers. In order to maximize effectiveness, a comprehensive security program must be developed including a number of prevention, awareness and security measures. No system or network can be totally secure against attack, especially a determined attack using the new more powerful workstations or mainframes, or from insiders, but a comprehensive security program can help reduce the risk tremendously. In a 1987 survey of 368 U.S. businesses, only 44 percent reported using computer security devices, and in retail and finance,

30 percent had not defined computer security responsibility, not very encouraging statistics.[1]

The DOD and the National Security Agency (NSA) have been put in charge of the national effort to ensure network security in combating viruses and network terrorists for the government and the private sector.[2] These two organizations have the most experience in communications security and have jointly established the National Computer Security Center at Ft. Meade, Maryland to conduct research and search for solutions. The National Institute of Standards and Technology (NIST, formerly the National Bureau of Standards, NBS) has also been involved in developing security and encryption standards, clashing at times with the DOD and NSA. Some people feel that the viewpoints taken by the DOD and NSA are not in-line with the needs of the private sector.

> NSA's model doesn't adequately address the need for maintaining data integrity, says Dr. David Clark, researcher at MIT's Laboratory for Computer Science, it isn't sufficient for commercial environments because it is more focused on access controls and preventing unauthorized disclosure of information.[3]

What I see here is, in reality, a fight over research funds, the government is trying to utilize its resources more effectively, rather than splitting its efforts in the area, which would be more costly. The

NIST currently "states that virus research has a low priority, as accidents, errors, earthquakes, floods, and fires are more prevalent and more important," but in reality they just do not have the resources (money and people) to effectively do the job.[4] Part of the criticism stems from NSA being a super-secretive organization, and it would be a lot easier for private researchers, such as Dr. Clark, to gain access to anything the NIST may happen to be working on or any dramatic discoveries. NSA has a strict "need to know" policy on security of information and how it operates, which precludes open access by private researchers, but that does not mean they cannot do the job. Resources need to be efficiently used to develop the best ways to protect the networks against abuse and criminal behavior.

Computer crime is almost the perfect type of crime as it is so hard to trace, especially in an interconnected network with hundreds or possibly thousands of users. Ways to trace do exist in most large computers (mini and mainframes), which produce an audit trail analysis of traffic. This information is supposed to be used by the systems operation and maintenance personnel to monitor the status of the network computer, its relative traffic load and help

in designing future networks. It is also useful in tracking down the source of an infiltration. Depending on the sophistication of the infiltrator, it may be possible to determine how the person entered the network, what damage he caused, and hopefully leave a trail that will lead to his apprehension. It sounds fairly simple, but doing audit tracking is a very time-consuming, tedious task that involves many man-hours of time as it usually all done by hand because you do not really know what you are looking for or where to find it. In a large network there may be huge volumes of information at various sites that would have to be sorted through, plus many times infiltrators will enter various networks before getting to the target network to cover their trail. It took 18 months of work for Dr. Stoll to catch the hackers in the NASA and Lawrence Livermore systems, and only then by enticing him to stay connected for a long time and tracing an active call. A one-time incursion to destroy, launch a virus or plant a trojan horse, would be nearly impossible to trace, and usually would be too late to prevent any damage. Audit trails are not part of a PC's standard equipment, and with the proliferation of local and wide area networks of PC's, a valuable tool against

crime is lost. Any PC network would have to have special (cost prohibitive in most cases) devices attached to perform the audit function. Database programs, such as IBM's dBase2, do not have the capability to readily provide an audit trail analysis, plus due to the innate user friendliness and ease of access of the program, it has a multitude of security problems (it is very susceptable to infiltration and manipulation).[5] IBM is still working on correcting these problems, but it is not easy without seriously changing the usefulness and ease of use of the program. IBM's updated database management program, dBase3, does not fare any better as it has some of the same design flaws of dBase2, but IBM is working to correct them through program patches.[6] These two database programs are very versatile and prolific throughout the computing world.

Viral Defenses

Are there any safeguards against network terrorists and insiders who use computer viruses? There has been a lot of discussion on the security aspects and what organizations and people can do to protect themselves from this plague. Coincidentally, when computer viruses really began to take off and

became highly publicized in the media, industry saw the rapid introduction of the "vaccine." Vaccines have been marketed as the "cure" for what ails your system and that they can even prevent a virus from entering your system. Vaccines are virus-specific, in other words, one vaccine may be good against one or several viruses, but not against all varieties. For example, Ferret was developed specifically to find and destroy the Scores virus, which may have been the worst virus to hit Macintoshes so far, but would not work against any other virus.[7] And according to industry experts, few perform as promised and others can disrupt programs or even destroy data.[8] Dr. Harold Joseph Highland, editor of the journal on Computers and Security, said that there are several programs on the market claiming to counteract viruses, but "no one should expect total protection."[9] He has received numerous requests from vaccine manufacturers to send them all the viruses he has so they can test their products, with the most amusing being a new entrant to the field who wanted at least one virus just to make sure his product worked, (after it was already on the market!).[10] He and Dr. Fredrick Cohen, a noted expert on computer viruses, have taken a strong stance on not distributing viruses, and

especially look askance to some vaccine manufacturers who have been intentionally distributing viruses to potential customers to drum-up business.[11] Most vaccines concentrate on protecting the first twelve sectors of a disk, which carry most of the critical information, plus the operating system in the next 196 sectors on a bootable disk. Some work on protecting the command.com, or any *.com or *.exe commands by recognizing any attempt to write to the command or recognizing any of a few specific interrupt calls.[12] These vaccines therefore prohibit authorized users from doing legitimate operations, such as rebooting the system in the event of a lock-up or formatting a disk. Some vaccines attempt to screen any viruses trying to enter the system by accepting only approved programs, doing a check for known virus strains or by inspecting a known clean system back-up and checking the current program against it to see if any modifications have been made.[13] Any variations cause the system to stop processing and lock-up until an operator intervenes in the situation. Some vaccines will create a software barrier to the virus' replication and malicious acts and warn the user that an unauthorized attempt has been made to access the system, while others will not only detect and warn,

but attempt to erradicate the vermin. A fairly complex program called check-sum, "is a program to form a cryptographic checksum of files in a computer system in order to allow their integrity to be checked at will."[14] This will allow all disk files to be check instead of just a few.

> Flushot Plus (10K RAM minimum) includes approved TSR list, write-protection for files, read protection for files, signature check, run-time signature check, hard disk access lock-out, FAT copy and CMOS copy.[15]

Again, a fairly complex checking system to try to avoid infection, or at least allow recovery of the critical sectors of the disk in case of a virus. Alarms are a variation of the vaccine and work to alert the user of an unauthorized entry into the system. This can be useful in detecting a trespasser or spy and immediately shutting down the network and mobilizing resources to catch the interloper. With the destructive virus, though, the warning would be too little, too late as with computer-like speed the virus can lock-up the network and destroy valuable data. Also, if the alarm causes the network to shut itself down or be shut down by system operators, to prevent any damage, that just may the goal of the terrorist, to disrupt the system and prevent it from operating. Taking a network down can be just as

devastating to its function as a destructive virus can be to data. Alarms alone offer little security.

How effective are vaccines? And at what cost do we employ them? "Currently there is no foolproof way to defend against software vandalism."[16] Vaccines will give people an added measure of security, but there are no guarantees, there are just too many virus strains and mutations for any anti-viral program to be 100 percent effective. And none claim to be, but they can be useful in a coordinated effort to fight viruses and other infiltrations. Many people complain that all these vaccines are an unwanted inconvenience, irritating as they make the simplest commands difficult (formatting a disk), time consuming and costly in terms of data space storage and productivity.[17] The checksum program, for example, adds an additional 4.5K bytes to each program, Vaccine 1.2K (384K RAM minimum), will increase your boot-up time by several minutes and any attempt to recompile a program will be flagged as a "virus-type" activity and stopped.[18] Vaccines can be overridden or just turned off by users who do not want the hassle or wasted time, and just as with any security device, it can only work when used properly. Otherwise, the protection device is useless and the system becomes

vulnerable. Manufacturers will continue to develop and market the newest in software protection, but vaccines will have to evolve quickly to keep pace with the ever-increasing number of new virus mutations being created. In 1988, Dr. Highland, called the computer viruses floating around today are of the "kindergarten" variety; the newer breed are more sophisticated; most existing virus filters (vaccines) may be helpless against them.[19] With the development of new countermeasures, virus creators work just as feverently to overcome and defeat them.

In addition to the vaccines, there are a few hardware protection devices. A new virus filter called "Disk Defender monitors the signals between the computer and the drive to intercept unwanted write commands," and informs the user of any attempts and the disk-protect status.[20]

> One approach suggests that the absolute isolation of a virus in the Intel Corp, 80386 microchip environment is possible because a 386 machine can be partitioned into numerous virtual machines. This capability supposedly keeps material from one part of the machine from moving to another part.[21]

There are very few hardware solutions as most companies want free and open architecture, especially those manufacturing the "clone-type" machines. Security devices raise the cost of the machines and

can make them incompatible with other machines of the same line.

Establishing private networks, (basically isolating your system from outsiders) is an effective tactic and is always an option (although very costly) for systems that require the utmost of security. These networks would have dedicated lines without dial-up capability, and in most cases end-to-end or link encryption. The network would be fairly secure against any outsider attack, but not safe from the corrupt insider. If an outsider were to determine which lines to tap into, the encryption should be effective in repelling the attack. In the competitive business world, private networks are very expensive to operate and maintain, plus for smaller corporations, the majority of the ones in the U.S. today, private networks are cost prohibitive, so they must opt for a public network and all the inherent vulnerabilities. Public networks are more economical for the small user and some do offer some protection against hackers and viruses, but none can be completely secure. Related to the idea of a private isolated network is the use of isolated back-up systems of the systems' most vital computers, memory and programs. Back-ups are very useful in the event of a catastrophic accident or

disruption to the network, but viruses that are timed to activate at a later date may be able to sidetrack this defense as they can be copied onto the back-up system, and then both copies are infected. Also, before any back-up system, program or disk is used the user must first be sure that the network is "clean" of the virus or else the virus will compromise that system. Backing up programs and data is always a good idea and in most cases is done automatically by the system. A back-up system though may not be and affordable option. However, private networks and back-up systems can help isolate the dangers of being infiltrated, as the ARPANET has been so many times, and that is fine if the company can afford to operate by itself. If the user needs to use public networks due to cost, the need to contact mobile remote sites or the need to share and exchange information among many varied and changing users, isolation can be very lonely.

Passwords

Password security into the network is another measure that can help improve security, if properly managed, which is most often not the case. Many times people will use passwords that are very easy to guess,

such as names of family members, birthdays, social security numbers, variations of the document name, or common words. Why? Because this makes the passwords easier to remember, and if that does not work, some people actually tape their password to their computers or post them on a central bulletin board. This defeats the entire security and authentification system, making it harder for the security manager to do his job, but easier for the network terrorist and insiders to do theirs. Passwords, to be effective in guarding the system and positively identifying all users of the system must be kept secret, changed on a frequent basis (more than once a year), be random including either numbers or punctuation marks, and be in encrypted form when stored in the computer. The biggest stumbling block to password security is not technical, but people and their bad habits and lax attitudes toward security in general. People using the computer and network must be aware of the dangers and be willing to accept harder to memorize passwords that will change often, a difficult task indeed. Two key points that are often overlooked, to the detriment of security are the installed passwords that come with the system and the changing of access codes and the deletion of the passwords of ex-employees. Computer

and communication device manufacturers often build-in passwords with their systems, and specifically tell the user to ensure that these are changed, but many people neglect to change them. An open door is left for anyone wanting to access the system and since some of these passwords are for system maintenance, they give the user access with extraordinary abilities to wreak havoc. This was the case for the German hackers, who used many manufacturers maintenance manuals to glean passwords, which are printed in the manuals! If an employee has been fired or quits, his access must be immediately cut-off, and his passwords deleted. People again fail to do this allowing a disgruntled ex-employee to re-enter the system and steal or destroy data. But even the most secure system can be overcome, if for example, the person being fired is the security officer or system programmer with the responsibility for managing the password files. They could install a hidden "back-door" password to enter the system at a later date, as in the Burleson case at USPA (ref Chap. III). Even if the person was not fired, but just an insider, many systems allow the system manager to have access to the password file, so he can pose as any other user

to abuse the system, and if his password is compromised so are all the others.[22]

Futuristic password schemes and devices are being developed to try to combat the increasing threat of compromise. One such device is hand-held and generates random passwords and is used after the user has logged onto the system with an initial fixed password.[23] The device's password allows the user to proceed to operate on the system, however many users were found to have written their initial fixed passwords right on the devices, making a lost one useless for security.[24] Again, user negligence could compromise a super system and cause a serious breach in security. Another device authorizes usage based on some personal attribute of the person, such as fingerprints, retina scans, voice prints and signature dynamics.[25] The field of study is called biometrics, and these devices offer great potential for secure user identification, but they too have their drawbacks. The main two are their high costs, and the problem of storing the identification data on all the machines for which a person has proper access.[26] The first problem will be overcome with time as the devices get mass produced, and the latter is being worked on with the advent of smart cards. Smart cards are very small

and contain a microprocessing chip on them that can store the biometric data of the user.[27] To use the system, the data on the card is checked against the person's characteristics right at the machine they wish to use. The card may be the wave of the future, it is simple to use and can only be used by the authorized user.

Encryption

Encryption within networks is another potential safeguard. Encryption is a viable and highly successful solution to keep out the casual hacker as it is too much of a challenge, and while encrypted the data is relatively secure. The process of encryption is the scrambling of the data via a very complex mathematical algorithm (called a cryptographic key) so that the data is unrecognizable and may only be reconfigured by someone holding the same cryptographic key. Without the key, the data cannot be read and privacy is protected from wiretaps, and so is the database if it is also kept in encrypted form. Encryption sounds like the cure-all for people's problems, but there are costs and drawbacks. Encryption is extremely expensive to obtain and operate, the devices require critical synchronization,

and keys must be changed on a periodic basis. Key changes require all members of the network to change their keys at the same time, but you will get mistakes, like people not changing the keys, using the wrong day's key, losing the keys and not destroying the used keys properly. Lost keys, keys stored in unsecure places and improperly destroyed keys will lead to a compromise of the network for those keys. Any data encrypted with those keys is therefore vulnerable, plus if a future key is compromised it can be used to infiltrate the network and possibly to inject a virus. These are common problems in using encryption, it goes back to the lax attitude of people about security. While some of the major corporations may be able to use encryption, most small businesses cannot afford the equipment and the associated administrative costs either in terms of money or productivity. Some encyrption system use as much computer power to operate as the entire computer power of some small firms. Also, encryption slows down the network, makes it less flexible and more difficult for even legitimate users to access. For example, businesses with personnel that need to be mobile would not be able to link up with the corporate network from just any location.

The NIST has endorsed a government standard that has been reviewed and certified by the NSA for public sensitive data encryption. The standard is called the Data Encryption Standard (DES) and has been used since the late 1970's for commercial telecommunications and data processing.[28] The DES permutates the data, which scrambles the data and it shifts the data, which moves the data's starting point, but retains the order.[29] Businesses and the federal government can use the DES to protect their sensitive data while in transit, however, it is not useful for the military as it is not secure enough for classified information. Some federal agencies use the DES, such as the Federal Reserve System and U.S. Treasury.[30] Recently the DES came under question as to vulnerability, as scientists have been able to, for the first time, crack the two prime roots of a 100-digit number, as

> several of the most secure cipher systems are based on the fact that large numbers are extremely difficult to factor even with powerful computers over a long time.[31]

The public key algorithm developed by Rivest, Shamir and Adleman, known as the RSA system, used extensively to transmit keys electronically, is encrypted by an algorithm that is based on the prime factors of 100-digit numbers and may be vulnerable from this type

of attack.[32] The effort involved hundreds of computers over three continents. Once the RSA algorithm has been cracked, the encryption key being transmitted is compromised, allowing unauthorized users to enter the network. As computers become more and more powerful, encryption algorithms will have to be periodically tested, recertified and revised to keep pace. Today, while possible, compromising any encryption algorithm is no easy task, so sophisticated infiltrators for the time being will use easier methods to try to overcome encrypted systems, such as stealing the security codes or by using "insiders".

The insider becomes a critical danger in an encrypted network; once decrypted all data is vulnerable. In addition, there is nothing to prevent the insider from inserting a virus from their terminal and have the virus be encrypted along with the data. This would make it especially difficult to track the virus, as all data would have to be decrypted in order to search for the virulent code. Encryption is not foolproof either, reference the ARPANET virus that rooted out encrypted passwords using the network's own encryption techniques. Defeating the insider is one of the most difficult if not impossible tasks, unless the entire operation is operated under prison type of

security and surveillance; a very expensive and socially unacceptable solution. The best that can be hoped for is to use preventive measures as described above to discourage any insider actions, run security checks for highly sensitive positions, and try to minimize the access needed by each person to minimize the amount of damage or theft they may be able to cause.

Personnel Security

Overall, the insider poses the most formidable threat to the network, and the hardest to identify, control or stop. This person has authorized access and who is to say that this person will go bad and destroy the system or steal from the database or abuse the network in some other manner. How can you identify the next corporate spy? The military and government try to do this through their security clearance investigation procedures, but with the huge numbers of people involved this can never be a foolproof method. A preventive measure that could be helpful is a security awareness program. The military developed its program many years ago and it is called the Communication Security Education Program (CSEP). The CSEP involves all areas of communication and

security. It has been weak on network and computer virus security, but these are relatively new threats and the program will be modified to incorporate them. Each person in the armed forces, including DOD civilians, must be briefed once a year on all areas of CSEP, also all new people to an organization receive an intense CSEP briefing. The CSEP manager has the responsibility to keep communications security at the forefront of each person's mind so that they think security when working. The manager not only gives a yearly briefing, but also is responsible for disseminating quarterly reminders, but many put out monthly awareness letters and bulletins. This type of program should be implemented in the commercial sector, which serves notice to the corporate insider that there are risks and the possibility of being caught is real and the consequences are unacceptable in tampering with the network or stealing information. The seriousness of security must be stressed to include the threat of legal prosecution of anyone intentionally misusing or abusing the system. Security awareness will not stop the determined individual, but could reduce the overall risk to the system.

Judicial and Congressional Actions

Computer crime laws are on the bocks in 21 different states, but when prosecuted, most attorney generals opt for a law such as larceny or embezzelment, rather than the computer crime laws. This is due to the difficulties in prosecuting someone under the computer crime statutes, there have been very few precedents, and lawyers have had a difficult time in just trying to identify what exactly is computer crime and intent. In Congressional testimony in 1983, Floyd I. Clarke, Deputy Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation (FBI), stated that "there does not exist one generally recognized and accepted definition as to what computer crime is."[33] He also commented on the reluctance to use computer crime laws,

> Generally speaking, the statutes most frequently used by the Department of Justice and the FBI to prosecute and investigate computer related crimes are fraud by wire, interstate transportation of stolen property, bank fraud and embezzelment, destruction of Government property, and theft of Government property.[34]

Hence, it is easy to understand the reluctance to use computer crime laws, they overlap into so many other different areas, which have existing statutes and precedents for prosecution, conviction and punishment. It is simplier for a lawyer, judge and jury to

understand embezzelment, without having to comprehend the computer processes involved. People are being tried for computer crimes, but the cases are rare.

An interesting network security case involved a man that is not even allowed to use the telephone except to call his wife, mother and lawyer due to his hacking abilities and fears that he has planted virus-type trojan horses and could activate them with a simple phone call.[35] Kevin Minick allegedly broke into a number of computer systems, stealing valuable computer programs and long distance phone services. He is the first person known to have been charged under a new federal law that prohibits breaking into an interstate computer network for criminal purposes.[36] He has a history of hacking, and some very coincidental circumstances following his run-ins with the law: the judge in the case had his credit rating mysteriously lowered, the telephone of Minick's probation officer was disconnected without any knowledge of the phone company, a false an damaging story was placed on a news wire service on a company that refused him a job, and the record of his offenses at age 17 disappeared from police computer records.[37]

Congress held hearings on the subject of computer security and privacy trying to determine the

nature of the problem and what direction Congress should take in trying to protect its own networks and databases from incursions and how to set the precedent for the commercial sector. What came out was there was little direction in the Federal Government. A 1986 study done by the OTA, showed that there is little or no oversight or consideration of the privacy implications of federal electronic record systems.[38] The OTA stated the Office of Management and Budget (OMB), which has the responsibility for computer security oversight in the federal government, has been lax in its duties.[39] In Congressional testimony on 26 Oct 83, then Deputy Director of OMB, Joseph Wright, did defend the past actions of OMB in trying to lead the awareness campaign, but he also agreed that OMB had to increase its efforts and stress the imperitiveness of computer security and privacy.[40] He also referred to the OMB Circular No. A-71 (released 27 Jul 78), entitled "Security of Federal Automated Information Systems," that details guidelines for computer management and computer security for all government agencies and departments.[41] In testimony in 1984, Mr. Wright, said that in addition to OMB Circular A-123 (released 23 Aug 83), entitled "Internal Control Systems," implementing the Federal

Managers' Financial Integrity Act (Public Law 97-255), they were in the process of updating the 1978 OMB Circular A-71.[42] Circular A-71, establishes a basic federal computer security program, which basically was a good document when released; circular A-123 provides internal control policy guidance in safeguarding assets from abuse and misuse.[43] However, as the OMB says it is doing a great job in improving the security of federal system, not all are in agreement.

> The GAO has been quite critical of OMB, basically stating that OMB has not assumed a strong leadership role in this field and they have indicated and urged OMB to revise its policy on computer security, and that OMB did not respond to the request.[44] Moreover, reports in 1983, of the President's Private Sector Survey on Cost Control, called for a stronger government-wide emphasis on information resources management and specifically for OMB to exercise more aggressive management leadership.[45]

Walter L. Anderson, Senior Associate Director, Information Management and Technology Division, GAO, stated in 1983, that even though the OMB has issued guidance, it does little in the way of follow-up to ensure compliance.[46] Two years later in 1985, not much had changed, as a GAO survey of 25 mission critical systems at 17 different agencies, overall "the results were that each of the systems were vulnerable to abuse, destruction, error, fraud, and waste."[47] The progress since 1985 has not been

substantial as borne out in a follow-up study done by the GAO in 1986-87, presented to Congress on 19 May 87. Thomas P. Giammo,, Associate Director, Information Management and Technology Division, GAO, stated,

> We found that the practices in use at all nine agencies [surveyed] had permitted decisions critical to the specification, design and construction of all nine systems to be made without adequate management consideration of important security issues. Consequently, we believe that the systems currently in development at many civilian agencies and intended to be used at least through the 1990's are likely to possess many of the same security deficiencies we had previously found in older systems. None of the agencies reviewed treated informtion security as one of the system's integral functional requirements.[48]

The U.S. civil government with few exceptions has not been able to get a handle on this problem, and this is a dangerous situation. In relation to databases, few laws exist, and an attempt to pass legislation in this area has failed. This is not the case in most European countries, as they have laws governing the use of government databases, and some include private databases.[49] In France, an overseeing commission on databases regularly steps in when it thinks cross-matching is getting out of hand, and has even required some mail-order companies to inform consumers when their names are transferred from one computerized list to another.[50] Congress has made some progress as

the hearings have publicized the extensiveness of the problem and have forced many government agencies to reevaluate their own security procedures and to include security and privacy considerations when procuring new systems. Not all measures are welcome, however. The Reagan Administration in early 1987 made several attempts to monitor the use of public databases as part of an effort to control access to unclassified, but sensitive information, but this policy was withdrawn under intense congressional pressure and fears the oversight would have given the government "Big Brother" control over all the computer systems in the country.[51]

Common sense is the last part of this overall security program. There are a number of preventive methods to try to combat the threats to networks, while some are inconvenient and time consuming, it is a lot harder to explain why a system is effectively dead and all data lost. The safest system is an isolated one that only has one user and no introduction of uncleared outside software. Of course, this could hamper one's creative freedom and productivity. The next best things for a user to do are to run virus checks regularly, not load "shareware" (free software available from a variety of

sources) from unknown sources, do not let others put their unchecked disks into your machine and visa-versa, make back-up copies of disks at regular intervals (may be the best bet), read the known virus and suspected software listings and use write-protect on floppy disks whenever practical.[52] In the business community all of the above measures should be followed whenever practical. In addition, do not let people bring in disks from home to use on company computers or home to use on home computers, do not allow any shareware from electronic bulletin boards, and try to minimize the amount of sharing of files to the minimum necessary for job accomplishment.[53] Another possibility is to test each disk prior to use on any company machines, but again this is time-consuming, inconvenient, and costly in money and productivity.[54] If connected to a data network, try to use a buffering system or have one isolated computer for that function so if it does get infected it will not infect the entire system, also turn off modems when they are not being used, and keep systems utilities off the system unless needed during that particular session. System utilities can be used to penetrate the system and can give the penetrator "super-user" capabilities.[55] There are drawbacks to all of these measures, but a

person or company must weigh the risk against the consequences and decide for themselves whether it is worth the extra time and money to be reasonably sure that the system is relatively secure. Infiltrators and insiders are able to avoid detection primarily because in many cases security had been sacrificed for productivity.[56] How much security is enough? It is a judgement decision that must be made after careful analysis of the potential risks to the system, the consequences of system failure or disclosure of data and the costs of properly securing the system (both monetary and productivity). This risk analysis must be realistic and coordinated throughout all members of the network, as it only takes one incident of insecure practices to introduce disaster. A major obstacle is that many computer centers do not have the expertise or resources to provide threat, vulnerability, and countermeasures analyses to their particular sites, much less risk assessments, security tests and evaluations, and disaster recovery plans.[57] The costs are high to protect systems, especially for small businesses or places just with PCs, but, clearly the cost of testing is justified when the potential loss is very high, taking into consideration the likelihood

of a loss occuring and the dollar value of that loss if it occurs.[58]

No solution in and of itself will be totally effective in deterring the network terrorist and insiders. What is needed is a comprehensive security program to include preventive measures and prosecution of perpetrators where possible. Security is not foolproof, and it is not cheap in terms of money, inconveniece and decreased productivity, but it may be worth it the one time it is needed. The computer and telecommunications industries need to develop security products and programs in earnest, companies and the government need to demand security measures be included in new products, and there is a need for more ethical behavior within the computer network.

NOTES - CHAPTER VI

[1] "U.S. Business Falls Short on Computer Security," Computers and Security, Apr 88, p. 210.

[2] Jeffery Chester, "Corporate, US Security Up For Grabs?" Infosystems, Jan 88, p. 24.

[3] Chester, p. 25.

[4] Eliot Marshall, "The Scourge of Computer Viruses," Science, 8 Apr 88, p. 134.

[5] Jean S. Bozman, "IBM Slow to Remedy Leaky DB2 Security," Computers and Security, Feb 88, p. 104.

[6] Bozman, p. 104.

[7] Suzanne Stefanac, "Mad Macs," Macworld, Nov 88, p. 95-98.

[8] Neil Munro, "Feds say Hackers Invaded Three Defense-Related Systems," Government Computer News, 19 Dec 88, p. 6.

[9] Gilliam Cribbs and Charles Arthur, "Pentagon Attacks Viruses," Computers and Security, Jun 88, p. 323

[10] Dr. Harold Joseph Highland, "How to Obtain a Computer Virus," Computers and Security, Aug 88, p. 337.

[11] Fredrick Cohen, "Ethical Issues in Computer Virus Distribution," Computers and Security, Aug 88, p. 335.

[12] Dr. Harold Joseph Highland, "How to Combat a Computer Virus," Computers and Security, Apr 88, pp. 161-2.

[13] Jim Seymour and Jonathan Matzkin, "Confronting the Growing Threat of Harmful Computer Software Viruses," PC Magazine (First Look), 28 Jun 88, p. 35.

[14] Dr. Harold Joseph Highland, "An Overview of 18 Virus Protection Products," Computers and Security, Apr 88, p. 159.

[15] Neil Rubenking, "Antivirus Programs Fight Data Loss," PC Magazine (First Look), 28 Jun 88, p. 36.

[16] "Fighting Parasites," The Futurist, Jul-Aug 88, p. 54.

[17] Seymour and Matzkin, p. 35.

Therese R. Welter, "Sick Computers," Industry Week, 15 Aug 88, p. 55.

[18] Highland, "An Overview of 18 Virus Protection Devices," p. 159.

Rubenking, p. 36.

[19] Dr. Harold Joseph Highland, "From the Editor," Computers and Security, Aug 88, p. 334.

[20] Highland, "An Overview of 18 Virus Protection Devices," p. 159.

[21] Belden Menkus, "No vaccine to ward off effects of virus attacks," Computerworld, 11 Jul 88, p. 58.

[22] Clifton H.C. Chan, "User Authentification During the Logon Process," in The New World Information Society, eds. J.M. Bennett and T. Pearcy, Holland: Elsevier Science Publishers, 1985, p. 863.

[23] Stephan Seldman, "Futuristic authentification schemes overcome passwords' limitations," Computerworld, 25 Nov 85, p. 58.

[24] Seldman, p. 58.

[25] Seldman, p. 58.

[26] Seldman, p. 58.

[27] Seldman, p. 58.

[28] Ronald J. Baum, "Cloak and Data," Security Management, Mar 89, p. 33A.

[29] Baum, p. 33A.

[30] Mitch Betts, Encryption Standard to get Reprieve, Computers and Security, Feb 88, p. 106.

[31] Malcom W. Brown, "Most Ferocious Math Problem is Tamed," Computers and Security, Feb 89, p. 76.

[32] Thomas Beth and Dieter Gollmann, "Algorithm Engineering for Public Key Algorithms," IEEE Journal on Selected Areas in Communications, May 89, p. 458.

Brown, p. 76.

[33] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1984), p. 414.

[34] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1984), p. 414.

[35] "Drop the Phone," Time, 9 Jan 89, p. 49.

[36] "Drop the Phone," Time, 9 Jan 89, p. 49.

[37] "Drop the Phone," Time, 9 Jan 89, p. 49.

[38] "Government Data Bases and Privacy", The Futurist, Sep-Oct 86, p. 53.

[39] "Government Data Bases and Privacy", The Futurist, Sep-Oct 86, p. 53.

[40] U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), p. 56.

[41] U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal

Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), p. 56.

U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), p. 8.

[42] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), pp. 8, 18-19, 110.

[43] U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), pp. 59, 99.

[44] U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), pp. 54, 98.

[45] U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), p. 99.

[46] U.S. Cong., Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1983), p. 100.

[47] U.S. Cong., House Subcommittee on Transportation Aviation and Materials and the Subcommittee on Science, Research and Technology of the Committee on Science and Technology, Federal Government Computer Security, Hearings, 99th Cong. 1st sess., (Washington, D.C.: GPO, 1986), pp. 3-4.

[48] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), pp. 3, 5.

[49] Anne Field, et al, "'Big Brother Inc.' May Be Closer Than You Thought," Business Week, 9 Feb 87, p. 86.

[50] Field, p. 86.

[51] Phillip Elmer-DeWitt, "Can a System Keep a Secret?" Time, 6 Apr 87, p. 69.

[52] Linda Bridges, "Computer Viruses Strike Colleges and Companies, Leaving Them Defensive," PC Week, 14 Jun 88.

David Stang, "Security Habits Build Healthy Software," Government Computer News, 27 May 88, pp. 53-4.

Arlan Levitan, "The Trojan Wars," Compute!, Mar 88, p. 59.

Stefanac, pp. 96-101.

[53] Seymour and Matzkin, pp. 34-5.

[54] Welter, p. 55.

[55] Jack Wynn, "Meeting the Threat," American Banker, 2 Feb 89, p. 8.

[56] Howard R. Keough, "An Inside Job," Security Management, Mar 89, p. 15A.

[57] Keough, p. 15A.

[58] Welter, p. 55.

CHAPTER V

CONCLUSIONS

Network security is a serious issue and demands more than the cursorary action people have attributed to it in the past. The issue has been explored, studied, discussed and hyped in magazine articles, journals, conferences, and congressional hearings, but progress/action has been slow, incredibly slow when compared to the advances in telematics technology. The transformation of the world economy to the information age is becoming a reality, computers and telecommunications are merging and becoming eternally intermeshed, and there is no sign that the pace of advancement will abate. Telematics technology seems to be speeding right along, with the provision of more and more services, more user-friendly interfaces, and the drive toward standard interconnected networks. However, in all this paradise for the user there are dangers to the network that must be addressed. The development of security technology is not keeping pace. There is interest by the government and some firms, but for the most part the demand is for more and easier access,

and not for expensive, slow security devices. The drawbacks of possible lower productivity and the inconvenience of operating with these devices need to be realized and accepted by the users as necessary to ensure the network and proprietary data will be protected. Users need to understand the reasoning and the reality of the risks to the network far outweigh the drawbacks.

> One of the costs of our success [in computing and networking] is that we are now in a position where misuse of our national and private computer networks can have a serious on the nation's economic, defense and social health.[1]

The dangers of the network terrorist and the insider are real and growing, and their instruments of havoc are becoming more sophisticated, more powerful and harder to prevent, detect and stop. Computer workstations have enormous computing capabilities, with as much power as many mainframes of only a few years ago, and of many that are still in operation today. The media has publicized the reported cases of computer viruses, but many other major breaches go unreported. They are not reported due to fear of loss of reputation or business, and lack of understanding as to how the infiltration occurred and how to prevent others from doing the same. The major networks of the U.S. must be protected and access controlled to

prevent a new wave of terrorist actions that may be more detrimental to national security than the current physical random actions of fanatical groups. The electronic "network terrorist" must be discouraged and inhibited from gaining access. The most insidious threat is that of the insider. This is a person entrusted to protect the integrity of the network and the associated databases, and they betray that trust by either destroying the network or stealing valuable and private data. Increases in security measures and awareness programs as outlined in the previous chapter will help deter most insiders, but more (besides a technological solution) still needs to be done to prevent a serious compromise in security. People must change.

In combating the network terrorist, the insider and computer viruses, technology is limited in its options, especially when the pace of advancement in computing power, telecommunications and their uses is far outstripping the development of security devices to ensure a safe network. Telecommunications magazine, Jan 89 issue, listed three areas of network management development, with the "traditional areas" of how to operate the network; "new areas" on system management and asset management; and "emerging areas"

of directory and security management.[2] Infiltrators are finding ways to enter the network and compromise systems faster than computer system managers can find ways to stop them. In order for security programs and technological solutions outlined in Chapter IV to be effective, I believe we need to change people's attitudes toward security. Users need to demand more security measures be built-in standard in their machines and push for technological advancements in security from manufacturers to keep pace with the increases in computing power and sophistication of the threats; they must be willing to accept the associated losses in computing speed and ability; and probably the most critical, they must change the attitude that security is not a real issue in today's telematics world. In order for a security program to work it must be accepted, believed in and implemented by the people using the network. If the attitudes toward security do not change, people will continue to be careless or actively turn off and by-pass security measures as inconvenient, aggravating annoyances. In congressional testimony, Thomas P. Giammo, Associate Director, Information Management and Technology Division, General Accounting Office, stated the difference between the Defense Department and other

agencies is the basic attitude of security is built-in with specific standards and guidelines, it is considered part of the entire development process for any new system.[3] To which Congressman Robert S. Walker of Pennsylvania responded, you may lay out the guidelines, but if you don't change the attitudes, even though guidelines exist, they will be ignored as much as possible.[4]

Users need to stress to their network managers and telecommunications managers the need for security of their data. Users should perform a risk assessment of their systems to determine their weaknesses and whether they would continue to survive if all systems were lost and whether data privacy is a key issue. If the risk assessment determines the system warrants protection, a comprehensive, and not a piecemeal, security plan must be implemented. This includes demanding security measures be installed by the manufacturer. Presently, computer manufacturers will continue to provide what the majority of users want: free and open access with very costly security devices added only on a case-by-case basis. The scarcity of demand for standard security measures is delaying the development and mass production of newer, more improved built-in security devices. The delay will

perpetuate itself until manufacturers feel the demand is strong enough and the potential profits in security devices are reality. Security devices are expensive, and competitive and fiscal pressures (especially in the government) dictate the system consist of the minimum operations and security needed, but this may eventually mean disaster for the user and the privacy of individuals. It is a catch-22 situation that may be resolved, unfortunately, by a publicized major destructive infiltration or disruption of a critical network that could have been avoided if proper security devices were in place. Users may realize after a disaster that the threats are real, but that is not the concern in today's booming information age.

Securing a system contradicts the basic premise of an information society, of standard open networks with the free and easy access and sharing of information. Security systems slow down the system and make it more difficult for even legitimate users to gain access. Most people want a user friendly system that is responsive and not literally more work to use than if the job was done manually. We, as a society, have been engrained with the premise, especially after World War II, that machines are built to make work easier for us, not to be a stumbling

block. This way of thinking in and of itself is a stumbling block to security devices, and must be modified. It is a real dilemma, a free and open (and vulnerable) society of computer networks, or secure, isolated private networks with limited access. A compromise must be reached, or a real longshot, trust and honesty must dominate our society.

Security would not be necessary if people were completely honest and trustworthy. The proposed solutions and preventive measures may help improve security, but the mechanical and technological solutions miss the crux of the problem. The problem is people and their attitudes toward computer-crime and security. Ethical behavior in the network, where consideration and respect are revered would do more for security and productivity than any hardware device. It just takes that one incident, that one person to ruin it for everyone by putting the fear of a devastating attack in everyone's mind so that they are fearful of using the network. Congress has been looking at computer crime legislation to prosecute the infiltrators; after the damage is done.

> Probably more important than new laws to criminal prosecutions in deterring hackers from virus-related conduct would be a stronger ethical code among computer professionals and better internal policies at private firms, universities and government institutions to

> regulate the usage of computing resources. If hackers cannot win the admiration of their collegues when they succeed at their clever stunts, they may be less likely to do them in the first place.[5]

Early in the development of computers, the number of operators and users was small. These people developed a respect for and an ethical stance for using the computer. This all began to change as computers began to proliferate, and has even expanded more due to the revolutions made in telecommunications. Today there are millions of computer users, many interconnected across the nation and all over the world. The small clique of users has been lost, but their principles of ethical operations and respect may be salvaged. Ethics is not only a problem in the telematics world, but also in business, in the government and in the military. The military has been trying to resolve the problem by the use of auxillary professional military education that includes teachings on ethics. This may also hold possibilities for the public and rest of government. David J. Farber, Chair of Division Advisory Panel of the National Science Foundation Division of Networking and Communications Research and Infrastructure stated that the panel deplored what they called "a breach of ethics" by the 2 Nov 88 ARPANET incident, and he encourages all organizations managing and operating

networks to adopt and publicize policies and standards for ethical behavior.[6] Ethical codes and standards do exist and are published by professional computer associations, such as the Institute for Certification of Computer Professionals and the Data Processing Management Association. The Institute published a code of ethics conduct and good practices for computer professional in 1977.[7] (See Appendix B) The code specified what was acceptable behavior to become and remain a certified member of the Institute.[8] The code was very well written, and contained many tenets of trust and honesty that characterize a "professional", but this was before the boom in PCs, when the computer professionals were still a relatively small enclave. Not many computer users today are really interested in applying for certification from the Institute, but possibly interest may be peaked if these standards were introduced early in the computer user's life, through the school system. The Data Processing Management Association has gone a step further in publicizing and marketing its code of ethics, by including it in their management assistance program.[9] Computers are currently being used throughout the education system from elementary school to college, and if ethical usage could be taught and stressed

throughout the school years, possibly the principles would not be lost. This is a long range solution that will lay a foundation for the future, for the future holds the most potential for disaster as we become more and more dependent on these machines and the networks that interconnect them. Congressman Timothy Wirth of Colorado, testified his belief is Congress should pass legislation in the computer crime area, but that more is necessary. He stated,

> In our efforts to bring computer technology into our school systems, we should make a discussion of "computer ethics" an integral part of the curriculum. Just as driver's education helps to equip our nation's young people to be safe and responsible drivers, too should a computer ethics curriculum equip our young people to use a computer responsibly.[10]

The Massachusetts' Institute of Technology has tried to do just that in Project Athena; their computer system for use by the students. The system differs from other university systems as it has assumed that one of its responsibilities is to open a discussion of ethical use with its user community. The primary action that Project Athena has taken is publication of a set of principles.[11] The principles insist each user adhere to certain standards of conduct, mainly to use the system in an ethical, honest and professional manner. This alone will not solve the problem, but it is a step in the right direction. Value changing is a

slow, long, and very difficult process, but it must be tried and hopefully for the new generation of users it will be successful.

So what kind of world do we have to look forward to? The information systems explosion has been a boon to mankind, but will the inconsiderate deliberate acts of a few hold us back in creativity and productivity? Will fear and paranoia dominate society? Or will the telecommunications and computer industries develop an intelligent system or hardware or software solution that will negate the effects or tricks of future network terrorists, whose methods most certainly be much more sophisticated especially with the advent of the workstations that put the power of a mainframe computer in a portable desktop model? These are tough questions, but need to be explored and not glossed over. We need to keep the spectre alive of the possibility one of our critical systems may become the target of a network terrorist or another country. The potential is there and the stakes are very high as we depend more and more on telecommunications and computers; we cannot lose sight that with every benefit to mankind there are always detracters and those that will take advantage of it for their own self-centered and malicious purposes.

Networking is a risky venture, and presently our networks and databases are very vulnerable to infiltration. Security must remain foremost in the minds of the users everyday, and attitudes toward security have to change if we are to protect our future. In the military, my own unique perspective, today many of the top military leaders play simulated war games on computers using many differing scenarios, however the next war may just be fought on an electronic battlefield, computer vs computer with just as devastating results to our society and its freedoms.

NOTES - CHAPTER V

[1] David J. Farber, "NSF Poses Code of Networking Ethics," Communications of the ACM, Jun 89, p. 688.

[2] Vince Barrett, "Future Scenarios for Network Management," Telecommunications, Jan 89, p. 66.

[3] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), pp. 10-11.

[4] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security, Hearings, 100th Cong. 1st sess., (Washington, D.C.: GPO, 1987), pp. 10-11.

[5] Pamela Samuelson, "Can Hackers Be Sued for Damages Caused by Computer Viruses", Communications of the ACM, Jun 89, p. 668.

[6] Farber, p. 688.

[7] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), p. 95.

[8] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), pp. 94-9.

[9] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), p. 103.

[10] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 1st sess., (Washington, D.C.: GPO, 1984), pp. 10-11.

[11] Jerome H. Saltzer, "Teaching Students About Responsible Use of Computers," Communications of the ACM, Jun 89, p. 704.

BIBLIOGRAPHY

Adams, Danny E. "U.S. Telecommunications Policy: Directions for the Next Five Years." IEEE Communications Magazine, Jan 89, pp. 43-53.

Barrett, Vince. "Future Scenarios for Network Management." Telecommunications, Jan 89, pp. 65-6, 85.

Baughman, Alan and Faulhaber, Gerald. Telecommunications Access and Public Policy. Norwood, N.J.: Ablex Publishing Co., 1984.

Baum, Ronald J. "Cloak and Data." Security Management, Mar 89, p. 33A-35A.

Benbow, Gary. "Data Privacy - The Cost of Freedom." Computers and Security, Feb 89, p. 75.

Berniker, Mark D. "Electronic mail now links Soviets, U.S." Daily Camera, Business Plus Section, 14 Mar 89, p. 9.

Bequai, Esq., August. The Cashless Society: EFTS at the Crossroads. New York: John Wiley & Sons Publishing Co., 1981.

Beth, Thomas and Gollmann, Dieter. "Algorithm Engineering for Public Key Algorithms.' IEEE Journal on Selected Areas in Communications, May 89, pp. 458-64.

Betts, Mitch. "Encryption Standard to get Reprieve." Computers and Security, Feb 88, p. 106.

Boyd, Robert S. "Into the Information Age." Daily Camera, Business Plus Section, 28 Feb 89, pp. 1, 12.

----------. "Make way for computer shopping, private satellites and interactive videos." Daily Camera, Business Plus Section, 28 Feb 89, p. 13.

Bozman, Jean S. "IBM Slow to Remedy Leaky DB2 Security." Computers and Security, Feb 88, p. 104.

Bridges, Linda. "Computer Viruses Strike Colleges and Companies, Leaving Them Defensive." PC Week, 14 Jun 88, pp. 19-20.

Brown, Malcom W. "Most Ferocious Math Problem is Tamed." Computers and Security, Feb 89, p. 76.

Campbell, Douglas E. "The Intelligent Threat." Security Management, Mar 89, pp. 19A-22A.

Castro, Lawrence. "An Overview of the DOD Computer Security RDT&E Program." Proceedings of the 10th National Computer Security Conference, 21-24 Sep 87, pp. 263-5.

Chan, Clifton H.C. "User Authentification During the Logon Process." In The New World Information Society. Eds. J.M. Bennett and T. Pearcy. Holland: Elsevier Science Publishers, 1985, pp. 860-5.

Chester, Jeffrey. "Corporate, US Security Up For Grabs?" Infosystems, Jan 88, pp. 24-5.

Cohen, Fredrick. "Ethical Issues in Computer Virus Distribution." Computers and Security, Aug 88, pp. 335-6.

Cornett, Linda. "CU students likes doctors in finding computer cure." The Daily Camera, 5 Nov 88, pp. 1A, 10A.

Cribbs, Gilliam and Arthur, Charles. "Pentagon Attacks Viruses." Computers and Security, Jun 88, p. 323.

Denning, Peter J. "The Science of Computing." American Scientist, Mar-Apr 89, pp. 126-8.

Dickman, Steven. "Hackers revealed as spies." Nature, 9 Mar 89, p. 108.

Eisenberg, Ted et al. "The Cornell Commission: On Morris and the Worm." Communications of the ACM, Jun 89, pp. 706-9.

Elmer-DeWitt, Phillip. "Can a System Keep a Secret?" Time, 6 Apr 87, pp. 68-9.

----------. "Invasion of the Data Snatchers." Time, 26 Sep 88, pp. 62-7.

----------. "The Kid Put Us Out of Action." Time, 4 Nov 88, p. 76.

Farber, David J. "NSF Poses Code of Networking Ethics." Communications of the ACM, Jun 89, p. 688.

Fawn, David. Telecommunications Seminar speaker from Southwestern Bell. Univ. of Colorado at Boulder, 5 Apr 89.

Field, Anne et al. "'Big Brother Inc.' May Be Closer Than You Thought." Business Week, 9 Feb 87, pp. 84-6.

Gait, Jason. "Communications Security for Electronic Funds Transfer Systems." IEEE Journal on Selected Areas in Communcations, May 84, pp. 414-22.

Geller, Henry. "Telecommunications Policy Issues: The New Money Delivery Modes." in Electronic Funds Transfer and Payments: the Public Policy Issues. ed. Elinor H. Solomon. Boston: Kluwer Nijhoff Publishing Co., 1987, p. 63-78.

Hafner, Katherine. "Is Your Computer Secure?" Business Week, 1 Aug 88, pp. 64-72.

Halal, William. "Computer Viruses: The 'AIDS' Of The Information Age?" The Futurist, Sep-Oct 88, p. 60.

Highland, Dr. Harold Joseph. "An Overview of 18 Virus Protection Products." Computers and Security, Apr 88, pp. 157-61.

----------. "From the Editor." Computers and Security. Aug 88, p. 334.

----------. "How to Combat a Computer Virus." Computers and Security, Apr 88, pp. 157, 161-3.

----------. "How to Obtain a Computer Virus." Computers and Security, Aug 88, pp. 337-8.

----------. "Random Bits & Bytes," Computers and Security, Apr 88, pp. 117-26.

Irven, Judith et al. "Multimedia Information Services: A Laboratory Study." IEEE Communications Magazine, Jun 88, pp. 27-44.

Joyce, Edward J. "Time Bomb." Computer Decisions, Dec 88, pp. 38-43.

Karmin, Monroe with Sherrid, Pamela. "Risky Moments in the money markets." U.S. News and World Report, 2 Mar 87, pp. 44-5.

Karon, Paul. "The Hype Behind Computer Viruses: Their Bark May Be Worse Than Their 'Byte'." PC Week, 31 May 88, pp. 49, 53.

Keefe, Patricia. "It can't happen here...." Computerworld (Focus), 6 Apr 88, pp. 12-16.

Keough, Howard R. "An Inside Job." Security Management, Mar 89, pp. 13A-16A.

Latham, Daniel W. "Industry in Transition: Telecommunications--Yesterday, Today and Tomorrow." IEEE Communications Magazine, Jan 89, pp. 75-6.

Laudon, Kenneth C. and Laudon, Jane P. Management Information Systems, New York: Macmillan Publishing Co., 1988.

Levitan, Arlan. "The Trojan Wars." Compute!, Mar 88, p. 59.

Marbach, William D. et al. "Hacking Through NASA." Newsweek, 28 Sep 87, p. 38.

Markoff, John. "'Virus' in Military Computers Disrupts Systems Nationwide." New York Times, 4 Nov 88, p. A20.

Marshall, Eliot. "German Computer Spy Ring Broken." Science, 24 Mar 89, p. 1545.

----------. "The Scourge of Computer Viruses." Science, 8 Apr 88, pp. 133-4.

Martin, J. G. "Federal Reserve Communications System Planning." IEEE Journal on Selected Areas in Communcations, May 84, pp. 395-402.

McGowan, William G. "Investment in Telecommunications: Opportunities or Pitfalls in Today's Environment." IEEE Communications Magazine, Jan 89, pp. 29-31.

Menkus, Belden. "No vaccine to ward off effects of virus attacks." Computerworld, 11 Jul 88, p. 58.

----------. "U.S. Government Agencies Belatedly Address Information System Security Issues." Computers and Security, Aug 88, pp. 361-6.

Munro, Neil. "Feds say Hackers Invaded Three Defense-Related Systems." Government Computer News, 19 Dec 88, p. 6.

Murphy, Jamie. "A Threat from Malicious Software." Time, 4 Nov 85, p. 94.

Nash, J. Madeleine. "Power Station in a Pizza Box." Time, 24 Apr 89, p. 51.

O'Brien, Thomas J. "The Changing Face of DOD Security." Security Management, Jul 88, pp. 61-4.

Office of the Assistant Secretary of Defense. "DOD's 4 Year Virus Program." Computers and Security, Oct 88, pp. 446-7.

Ornstein, Severo M. "Beyond Worms." Communications of the ACM, Jun 89, pp. 672-3.

Peterzell, Jay. "Spying and Sabotage by Computer." Time, 20 Mar 89, pp. 25-6.

Pontine, Bob. "Some common sense about network viruses, and what to do about them." Data Communications, Apr 88, pp. 60, 62.

Qvortrup, Lars. Telematics. Philadelphia: J. Benjamins Publishing Co., 1984.

Richards, Evelyn and Smith, R. Jeffrey. "Hacker tracker followed trail across Atlantic." Daily Camera, 4 Mar 89, p. 11A.

Rubenking, Neil. "Antivirus Programs Fight Data Loss." PC Magazine (First Look), 28 Jun 88, p. 36.

Ruiz, Frank. "DOD Fights Off Computer Virus." Government Computer News, 5 Feb 88, pp. 1, 77.

Saltzer, Jerome H. "Teaching Students About Responsible Use of Computers." Communications of the ACM, Jun 89, p. 704.

Samuelson, Pamela. "Can Hackers Be Sued for Damages Caused by Computer Viruses." Communications of the ACM, Jun 89, p. 666-9.

Sanza, Richard. "Spying through Computers?" Newsweek, 10 Jun 85, p. 39

Seldman, Stephan. "Futuristic authentification schemes overcome passwords' limitations." Computerworld, 25 Nov 85, pp. 58, 67.

Seymour, Jim and Matzkin, Jonathan. "Confronting the Growing Threat of Harmful Computer Software Viruses." PC Magazine (First Look), 28 Jun 88, pp. 33-5.

Sharp, C.B.E., Sir Eric. "Global Networks." IEEE Communications Magazine, Jan 89, pp. 20-1.

Spafford, Eugene H. "Crisis and Aftermath." Communications of the ACM, Jun 89, pp. 678-87.

Staley, Delbert C. "Domestic Roadblocks to a Global Information Highway." IEEE Communications Magazine. Jan 89, pp. 24-5.

Stallings, Dr. William. "Interfacing to the Defense Data Network." Signal, Aug 88, pp. 103-7.

Stang, David. "Security Habits Build Healthy Software." Government Computer News, 27 May 88, pp. 53-4.

Stefanac, Suzanne. "Mad Macs." Macworld, Nov 88, pp. 93-101.

Sterling, Christopher and Thompson, Stephen. "The United States in International Communications." In International Telecommunications and

Information, ed. Christopher Sterling, Washington D.C.: Communications Press, 1984, pp. 1-13.

Sumner, Eric E. "Telecommunications Technology in the 1990s." Telecommunications, Jan 89, pp. 37-8.

Thornburg, David D. "Computer Viruses Use Networks to Spread the Disease of Distrust." Compute!, Jul 88, p. 10

----------. "The Global Village Under Siege-We've Met the Enemy and He Is Us." Compute!, Mar 89, p. 13.

U.S. Cong. Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computer Security in the Federal Government and the Private Sector. Hearings. 98th Cong. 1st sess. Washington, D.C.: GPO, 1983.

U.S. Cong. House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy. Hearings. 98th Cong. 1st sess. Washington, D.C.: GPO, 1984.

U.S. Cong. House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy. Hearings. 98th Cong. 2nd sess. Washington, D.C.: GPO, 1985.

U.S. Cong. House Subcommittee on Transportation Aviation and Materials and the Subcommittee on Science, Research and Technology of the Committee on Science and Technology, Federal Government Computer Security. Hearings. 99th Cong. 1st sess. Washington, D.C.: GPO, 1986.

U.S. Cong. House Subcommittee on Transportation Aviation and Materials of the Committee on Science, Space and Technology, GAO Survey, Federal Government Computer Security. Hearings. 100th Cong. 1st sess. Washington, D.C.: GPO, 1987.

Wells, Robert. "Solbourne Computer seeks to create workstation standard." Daily Camera, Business Plus Section, 17 Jan 89, pp. 10-11.

Welter, Therese R. "Sick Computers." Industry Week, 15 Aug 88, pp. 51, 55.

Westin, Alan F. "'We, the people' in the computer age." Computerworld, 14 Sep 87, pp. 73-80.

Wickham, Jr., John A. "Protecting Our Computers." Signal, Jan 89, pp. 17-19.

Wynn, Jack. "Meeting the Threat." American Banker, 2 Feb 89, p. 8.

"Another Infection." Time, 12 Dec 88, p. 33.

"Clever, Nasty and Definitely Antisocial." Newsweek, 14 Nov 88, pp. 24-5.

"Computer Viruses." The Colorado Engineer, Fall 88, pp. 8-9, 16-17. As transcribed from "Watch Out For Viruses" by Carl Thor. In PC Transmission, Apr 88.

"Drop the Phone." Time, 9 Jan 89, p. 49.

"Fighting Parasites." The Futurist, Jul-Aug 88, p. 54.

"Government Data Bases and Privacy." The Futurist Sep-Oct 86, pp. 52-3.

"How Deadly is the Computer Virus." Electrical World, Jul 88, pp. 35-6.

Newstrack, "Crime Statistics." Communications of the ACM, Jun 89, p. 657.

"Nothing to Sneeze At." Time, 11 Apr 88, p. 52

"Plugging Into City Hall." Time, 6 Mar 89, p. 33.

"U.S. Business Falls Short on Computer Security." Computers and Security, Apr 88, p. 210.

APPENDIX A

ANALYSIS OF A VIRUS[1]

Inside the Pakistani Virus

The Pakistani virus embeds itself within the boot sector of a disk. Using the disk view/edit utility of PC Tools it is possible to display the contents of that sector in hexadecimal code and the corresponding ASCII values (see Fig. A).

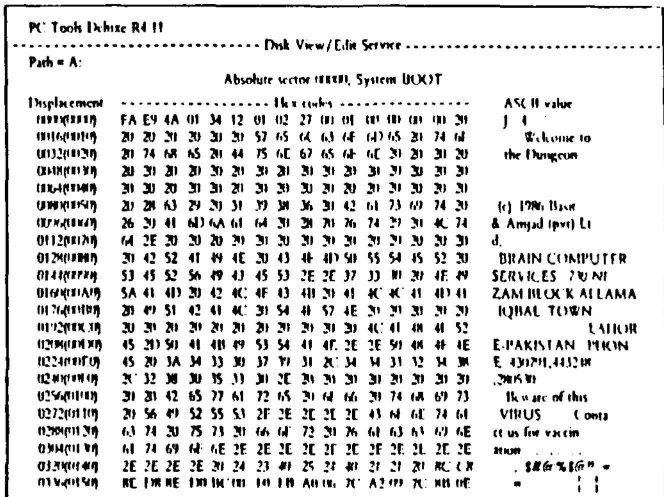

Fig. A.

A clear text version of the contents reveals the following:

Welcome to the Dungeon
© 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 Nizam Block Allama Iqbal Town
Lehore, Pakistan
Phone: 430791, 443248, 2800530
Beware of this VIRUS
Contact us for vaccination

The Alvi brothers, Basit and Amjad, sell compatible PCs in their store in Lehore. When contacted by a reporter for "The Chronicle of Higher Education," the 19-year old Basit Alvi admitted writing the virus and placing it on a disk in 1986 "for fun." He reportedly gave a copy of the virus program to a friend, another student. However, both brothers were at a loss in explaining how the virus emigrated to the States.

A map of an infected disk (see Fig. B) shows several hidden files beyond the normally hidden BIOS and DOS systems files as well as the three bad sectors, shown by "x" in the diagram. Although bad sectors are not readable under normal DOS procedures, using the same utility as was used to read the boot sector, we find parts of the warning announcement in these bad sectors (Fig. C on next page shows one portion of a bad sector).

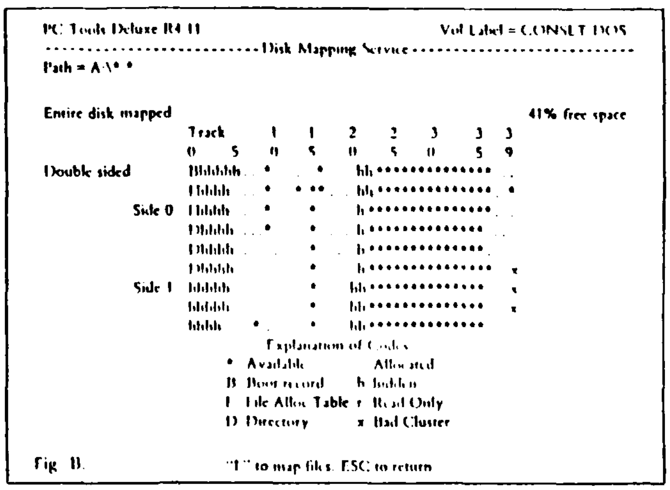

Fig. B.

PC Tools Deluxe R4.11

Disk View/Edit Service

Path = A

Absolute sector 00713, Cluster 00357

Displacement	Hex codes															ASCII value
0000(0000)	EB	26	28	63	29	20	31	39	38	36	20	42	61	73	69	74	&(c) 1986 (Basit
0016(0010)	20	26	20	41	6D	6A	61	64	73	20	28	70	76	74	29	20	& Amjad (pvt)
0032(0020)	4C	74	64	20	00	01	00	00	2E	C6	06	25	02	1F	33	C0	Ltd % v3+
0048(0030)	8E	D8	A1	4C	00	A3	B4	01	A1	4E	00	A3	B6	01	B8	76	L + N v

Fig. C.

NOTES - APPENDIX A

[1] Dr. Harold J. Highland, "Random Bits & Bytes," Computers and Security, Apr 88, pp. 119-120.

APPENDIX B

EXAMPLE CODE OF ETHICS[1]

INSTITUTE FOR CERTIFICATION OF COMPUTER PROFESSIONALS

codes

of ethics, conduct and good practice for certified computer professionals

Institute for Certification of Computer Professionals
35 East Wacker Drive
Chicago, Illinois 60601

Certified computer professionals are a select group of people who have qualified for and successfully completed an examination assessing their grasp of the knowledge considered by recognized experts as important to the area in which they are certified.

The ICCP has consistently, throughout its existence, recognized the need for a set of personal and professional standards to support and identify those individuals dedicated to the quest for knowledge and competence, to ethical behavior and social responsibility, and to the advancement of the computer profession. By choosing to seek certification, Certificate holders have demonstrated their concern for the continuing development of high standards of personal and professional conduct.

The following pages contain the Codes of Ethics, Conduct and Good Practice adopted by ICCP at its inception. *These Codes are guidelines to which all Certificate* holders subscribe and follow in the execution of their responsibilities.

ICCP also recognizes that violation of the Codes of Ethics, Conduct and Good Practice by any Certificate holder is an act contrary to the principles of the certification program and a breach of the requirements for certification. Therefore, the ICCP has reserved for and delegated to each Certification Council the right to revoke any Certificate issued under a Council's administration in the event that the Certificate holder violates the Codes of Ethics and/or Conduct or otherwise engages in conduct which is a discredit or disgrace to the computer profession. The revocation procedures approved by the Certification Councils are also included in this booklet.

The certification programs of ICCP represent a significant effort to promote high standards of excellence for members of the computer profession.

CODE OF ETHICS FOR CERTIFIED COMPUTER PROFESSIONALS

Certified computer professionals, consistent with their obligation to the public at large, should promote the understanding of data processing methods and procedures using every resource at their command.

Certified computer professionals have an obligation to their profession to uphold the high ideals and the level of personal knowledge certified by the Certificate held. They should also encourage the dissemination of knowledge pertaining to the development of the computer profession.

Certified computer professionals have an obligation to serve the interests of their employers and clients loyally, diligently, and honestly.

Certified computer professionals must not engage in any conduct or commit any act which is discreditable to the reputation or integrity of the computer profession.

Certified computer professionals must not imply that the Certificates which they hold are their sole claim to professional competence.

CODES OF CONDUCT AND GOOD PRACTICE FOR CERTIFIED COMPUTER PROFESSIONALS

The essential elements relating to conduct that identify a professional activity are:

A high standard of skill and knowledge.

A confidential relationship with people served.

Public reliance upon the standards of conduct and *established practice.*

The observance of an ethical code.

Therefore, these Codes have been formulated to strengthen the professional status of certified computer professionals.

1. Preamble

1.1: The basic issue, which may arise in connection with any ethical proceedings before a Certification Council, is whether a holder of a Certificate administered by that Council has acted in a manner which violates the Code of Ethics for certified computer professionals.

1.2: Therefore, the ICCP has elaborated the existing Code of Ethics by means of a Code of Conduct, which defines more specifically an individual's professional responsibility. This step was taken in recognition of questions and concerns as to what constitutes professional and ethical conduct in the computer profession.

1.3: The ICCP has reserved for and delegated to each Certification Council the right to revoke any Certificate which has been issued under its administration in the event that the recipient violates the Code of Ethics, as amplified by the Code of Conduct. The revocation proceedings are specified by rules governing the business of the Certification Council and provide for protection of the rights of any individual who may be subject to revocation of a Certificate held.

1.4: Insofar as violation of the Code of Conduct may be difficult to adjudicate, the ICCP has also promulgated a Code of Good Practice, the violation of which does not in itself constitute a reason to revoke a Certificate. However, any evidence concerning a serious and consistent breach of the Code of Good Practice may be considered as additional circumstantial evidence in any ethical proceedings before a Certification Council.

1.5: Whereas the Code of Conduct is of a fundamental nature, the Code of Good Practice is expected to be amended from time to time to accommodate changes in the social environment and to keep up with the development of the computer profession.

1.6: A Certification Council will not consider a complaint where the holder's conduct is already subject to legal proceedings. Any complaint will only be considered when the legal action is completed, or it is established that no legal proceedings will take place.

1.7: Recognizing that the language contained in all sections of either the Code of Conduct or the Code of Good Practice is subject to interpretations beyond those intended, the ICCP intends to confine all Codes to matters pertaining to personal actions of individual certified computer professionals in situations for which they can be held directly accountable without reasonable doubt.

2. Code of Conduct

2.1: Disclosure: Subject to the confidential relationships between oneself and one's employer or client, one is expected not to transmit information which one acquires during the practice of one's profession in any situation which may harm or seriously affect a third party.

2.2: Social Responsibility: One is expected to combat ignorance about information processing technology in those public areas where one's application can be expected to have an adverse social impact.

2.3: Conclusions and Opinions: One is expected to state a conclusion on a subject in one's field only when it can be demonstrated that it has been founded on adequate knowledge. One will state a qualified opinion when expressing a view in an area within one's professional competence but not supported by relevant facts.

2.4: Identification: One shall properly qualify oneself when expressing an opinion outside of one's professional competence in the event that such an opinion could be identified by a third party as expert testimony, or if by inference the opinion can be expected to be used improperly.

2.5: Integrity: One will not knowingly lay claims to competence one does not demonstrably possess.

2.6: Conflict of Interest: One shall act with strict impartiality when purporting to give independent advice. In the event that the advice given is currently or potentially influential to one's personal benefit, full and detailed disclosure of all relevant interests will be made at the time the advice is provided. One will not denigrate the honesty or competence of a fellow professional or a competitor, with intent to gain an unfair advantage.

2.7: Accountability: The degree of professional accountability for results will be dependent on the position held and the type of work performed. For instance:

A senior executive is accountable for the quality of work performed by all individuals the person supervises and for ensuring that recipients of information are fully aware of known limitations in the results provided.

The personal accountability of consultants and technical experts is especially important because of the positions of unique trust inherent in their advisory roles. Consequently, they are accountable for seeing to it that known limitations of their work are fully disclosed, documented, and explained.

2.8: Protection of Privacy: One shall have special regard for the potential effects of computer based systems on the right of privacy of individuals whether this is within one's own organization, among customers or suppliers, or in relation to the general public.

Because of the privileged capability of computer professionals to gain access to computerized files, especially strong strictures will be applied to those who have used their positions of trust to obtain information from computerized files for their personal gain.

Where it is possible that decisions can be made within a computer based system which could adversely affect the personal security, work, or career of an individual, the system design shall specifically provide for decision review by a responsible executive who will thus remain accountable and identifiable for that decision.

3. Code of Good Practice

3.1: Education: One has a special responsibility to keep oneself fully aware of developments in information processing technology relevant to one's current professional occupation. One will contribute to the interchange of technical and professional information by encouraging and participating in education activities directed both to fellow professionals and to the public at large. One will do all in one's power to further public understanding of computer systems. One will contribute to the growth of knowledge in the field to the extent that one's expertise, time, and position allow.

3.2: Personal Conduct: Insofar as one's personal and professional activities interact visibly to the same public, one is expected to apply the same high standards of behavior in one's personal life as are demanded in one's professional activities.

3.3: Competence: One shall at all times exercise technical and professional competence at least to the level one claims. One shall not deliberately withhold information in one's possession unless disclosure of that information could harm or seriously affect another party, or unless one is bound by a proper, clearly defined confidential relationship. One shall not deliberately destroy or diminish the value or effectiveness of a computer based system through acts of commission or omission.

3.4: Statements: One shall not make false or exaggerated statements as to the state of affairs existing or expected regarding any aspect of information technology or the use of computers.

In communicating with lay persons, one shall use general language whenever possible and shall not use technical terms or expressions unless there exist no adequate equivalents in the general language.

3.5: Discretion: One shall exercise maximum discretion in disclosing, or permitting to be disclosed, or using to one's own advantage, any information relating to the affairs of one's present or previous employers or clients.

3.6: Conflict of Interest: One shall not hold, assume, or consciously accept a position in which one's interests conflict or are likely to conflict with one's current duties unless that interest has been disclosed in advance to all parties involved.

3.7: Violations: One is expected to report violations of the Code, testify in ethical proceedings where one has expert or first hand knowledge, and serve on panels to judge complaints of violations of ethical conduct.

PROCEDURAL REQUIREMENTS FOR REVOCATION OF CERTIFICATE AWARDED

I. A Certification Council, on behalf of the Institute for Certification of Computer Professionals, has the right to revoke any Certificate which has been administered by it in the event that the recipient violates the Codes or engages in conduct which is a discredit or disgrace to the computer profession.

II. The grounds for revocation will be based upon the opinion of at least two-thirds of the members of the Council.

III. Procedure for handling revocation.

1. A formal written statement of charges alleging facts which constitute the grounds for revocation will be prepared.
2. A copy of said charges will be forwarded to the person accused, fixing a time within which such person may file with the Council answers to the charges.
3. If the charges are denied in the answer, the Council will fix a time for the hearing and give notice of the time and place of the hearing to the person accused.
4. Presentation of evidence in support of the charges will be made by the secretary (a non voting member) of the Certification Council.
5. Presentation of evidence in defense of the charges will be made by the accused or the designated representative of the accused.
6. Ample opportunity for both sides to present facts and arguments will be allowed at the hearing.
7. At the conclusion of the hearing, the Council will determine whether or not the charges have been sufficiently established by the evidence and whether the Certificate should be revoked or should not be revoked.
8. The accused will be notified of the decision by registered mail.
9. The accused has the right to request review of the decision by the Executive Committee of ICCP, provided an appeal in writing is submitted to the President, ICCP, within 30 days of the accused's receipt of the Council's decision.

NOTES - APPENDIX B

[1] U.S. Cong., House Subcommittee on Transportation Aviation and Materials of the Committee on Science and Technology, Computer and Communications Security and Privacy, Hearings, 98th Cong. 2nd sess., (Washington, D.C.: GPO, 1985), pp. 94-9.